IKIGAI LAW

Clause-wise mapping of the JPC report on India's data protection law

contact@ikigailaw.com | @ikigailaw

IKIGAI LAW

21 December 2021

CLAUSE-WISE MAPPING OF THE JPC'S RECOMMENDATIONS ON INDIA'S DATA PROTECTION LAW

This document compares the Personal Data Protection Bill, 2019,[1] introduced in the Parliament of India on 11 December 2019 (**Bill**) with the recommendations and changes proposed by the Joint Parliamentary Committee (**JPC**) in its report on the Bill, tabled in Parliament on 16 December 2021.[2]

The table below maps the provisions of the Bill and the JPC's recommended changes to the text of the Bill, with changes highlighted in yellow. The portions highlighted in yellow in the column titled 'JPC Recommended Bill Text' are changes to the Bill; deletions are represented by "(***)". Substantive changes and the JPC's remarks are listed in the column titled 'Changes and JPC Remarks'.

S. No.	Bill	JPC Recommended Bill Text	Changes and JPC remarks
		Long title and Preamble	
1.	***Long title*** To provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organisational and technical measures in processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data, remedies for unauthorised and harmful processing, and to establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto.	***Long title*** To provide for protection of the digital privacy of individuals relating to their personal data, to specify the flow and usage of (***) data, to create a relationship of trust between persons and entities processing the (***) data, to protect the rights of individuals whose (***) data are processed, to create a framework for organisational and technical measures in processing of data, to lay (***) down norms for social media platforms, cross-border transfer, accountability of entities processing (***) data, remedies for unauthorised and harmful processing, to ensure the interest and security of the State and to establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto	• The JPC considers the Bill as covering data as a whole, and hence, recommended removing references to "personal" data throughout the long title (para 2.11). • The long title adds "digital" before privacy since in the JPC's view, the Bill relates to privacy of information in the digital domain, and non-digitised data is not governed by the Bill. • The JPC believes that digital privacy must circumscribed and limited by the nation's sovereignty, integrity and state interest and security (para 2.12)

[1] The text of the bill is available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.
[2] The text of the JPC Report on the Personal Data Protection Bill is available at http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

2.	***Preamble*** WHEREAS the right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy; AND WHEREAS the growth of the digital economy has expanded the use of data as a critical means of communication between persons; AND WHEREAS it is necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation through digital governance and inclusion and for matters connected therewith or incidental thereto. BE it enacted by Parliament in the Seventieth Year of the Republic of India as follows:—	***Preamble*** WHEREAS the right to privacy is a fundamental right and it is necessary to protect personal data of an individual as an essential facet of informational privacy; AND WHEREAS the growth of the digital economy has expanded the use of data as a critical means of communication between persons; AND WHEREAS it is necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals that fosters sustainable growth of digital products and services and ensuring empowerment, progress and innovation through digital governance and inclusion and for matters connected therewith or incidental thereto. BE it enacted by Parliament in the Seventy-second Year of the Republic of India as follows:—	• The JPC proposes the changes in the Preamble to account for the heightened focus on the digital sphere and the regulation of the digitisation process (paras 2.8 and 2.12) • Despite noting suggestions that the Bill should focus on data protection rather than the digital economy (para 2.6), the JPC retains (and enhances) references to the digital economy.
	CHAPTER I: PRELIMINARY		
3.	***Clause 1: Short title and commencement*** (1) This Act may be called the Personal Data Protection Act, 2019. (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	***Clause 1: Short title and commencement.*** (1) This Act may be called the (***) Data Protection Act, 2021 (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	• The JPC recommends dropping personal from the title of the Bill, expanding its remit to cover the regulation of non-personal data ("**NPD**"). (para 2.15) • The JPC notes the challenges in separating personal and non-personal data in mass data transactions, the importance of protecting all data, and how restricting the legislation to

	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.	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.	only personal data hurts privacy. They propose a single regulator for simplicity and to account for any grey areas in anonymized and re-identified data. (paras 1.15.8.4 and 2.4) • Although no specific text has been provided, the JPC recommends a phased implementation of approximately 24 months for implementation of all or any provisions of the Act. It also calls for comprehensive analysis and consultation with stakeholders and emphasizes on keeping the legitimate business interests in mind. (para 1.15.9.6)
4.	***Clause 2: Application of Act to processing of personal data.*** The provisions of this Act,— (A) shall apply to— *(a)* the processing of personal data where such data has been collected, disclosed, shared or otherwise processed within the territory of India; *(b)* the processing of personal data by the State, any Indian company, any citizen of India or any person or body of persons incorporated or created under Indian law; *(c)* the processing of personal data by data fiduciaries or data processors not present within the territory of India, if such processing is— (i) in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India; or	***Clause 2: Application of Act to processing of personal data and non-personal data.*** The provisions of this Act shall apply to,– (A) (***) *(a)* the processing of personal data where such data has been collected, stored, disclosed, shared or otherwise processed within the territory of India; *(b)* the processing of personal data by (***) any person (***) under Indian law; *(c)* the processing of personal data by data fiduciaries or data processors not present within the territory of India, if such processing is— (i) in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India; or (ii) in connection with any activity which involves profiling of data principals within the territory of India; and	• The JPC notes that the core objective of the Bill is privacy and NPD should be protected to uphold privacy. NPD is added in the marginal heading to reflect the intent to regulate both personal and non-personal data. (paras 2.20, 2.22) • The JPC inserts "stored" in Clause 2(a) to make it more comprehensive. (para 2.24) • The JPC notes that the definition of person is exhaustive and the selective usage of the words "*State, any Indian company(…)*" is restrictive and might lead to complications. (para 2.23) • In the JPC's view, excluding anonymized data might encourage the manipulation or commercialization of data in the guise of anonymization, which will be detrimental to individual data privacy. Thus, the JPC

	(ii) in connection with any activity which involves profiling of data principals within the territory of India. (*B*) shall not apply to the processing of anonymised data, other than the anonymised data referred to in section 91.	*(d)* the processing of non-personal data including anonymised personal data. (B) (***)	recommends adding Clause 2(d) and modifying Clause 91 accordingly. (paras 2.21, 2.24)
5.	***Clause 3: Definitions.*** In this Act, unless the context otherwise requires,— (*1*) "**Adjudicating Officer**" means the Adjudicating Officer appointed as such under sub-section (*1*) of section 62; (*2*) "**anonymisation**" in relation to personal data, means such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Authority; (*3*) "**anonymised data**" means data which has undergone the process of anonymisation; (*4*) "**Appellate Tribunal**" means the Tribunal established under sub-section (*1*) or notified under sub-section (*4*) of section 67; (*5*) "**Authority**" means the Data Protection Authority of India established under sub-section (*1*) of section 41; (*6*) "**automated means**" means any equipment capable of operating automatically in response to instructions given for the purpose of processing data; (*7*) "**biometric data**" means facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological, or behavioural	***Clause 3: Definitions.*** In this Act, unless the context otherwise requires,— (*1*) **"Adjudicating Officer"** means the Adjudicating Officer appointed as such under sub-section (*1*) of section 63; (*2*) **"anonymisation"** in relation to personal data, means such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Authority; (*3*) **"anonymised data"** means data which has undergone the process of anonymisation; (*4*) "**Appellate Tribunal"** means the Tribunal established under sub-section (*1*) or notified under sub-section (*4*) of section 68; (*5*) **"Authority"** means the Data Protection Authority of India established under sub-section (*1*) of section 41; (*6*) **"automated means"** means any equipment capable of operating automatically in response to instructions given or otherwise for the purpose of processing data; (*7*) **"biometric data"** means facial images, fingerprints, iris scans or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological or behavioral	

	characteristics of a data principal, which allow or confirm the unique identification of that natural person; (*8*) "**child**" means a person who has not completed eighteen years of age; (*9*) "**code of practice**" means a code of practice issued by the Authority under section 50; (*10*) "**consent**" means the consent referred to in section 11;	characteristics of a data principal, which allow or confirm the unique identification of that natural person; (*8*) **"child"** means a person who has not completed eighteen years of age; (*9*) **"code of practice"** means a code of practice issued by the Authority under section 50; (*10*) **"consent"** means the consent referred to in section 11; *(11)* **"Consent Manager"** means a data fiduciary which enables a data principal to give, withdraw, review and manage his consent through an accessible, transparent and interoperable platform;	• The JPC recommends that the term "consent manager" which was defined as an explanation under Clause 23 of the Bill, be added to the definitions clause (para 2.28).
	(*11*) "**data**" includes a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means;	***(12)*** **"data"** includes a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means;	
	(*12*) "**data auditor**" means an independent data auditor referred to in section 29;	***(13)*** **"data auditor"** means a **(***)** data auditor referred to in section 29;	• The JPC finds that the word "independent" under the definition of data auditor under renumbered as Clause 3(13) is superfluous as it has been used in Clause 29. (para 2.29)
		(14) **"data breach"** includes personal data breach and non-personal data breach;	• The JPC recommends including the definition of "data breach", which had not been defined, even though it appears in various parts of the Bill. (para 2.30)
	(*13*) "**data fiduciary**" means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data; (*14*) "**data principal**" means the natural person to whom the personal data relates;	(*15*) **"data fiduciary"** means any person, including a State, a company, a non-government organisation, (***) juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data;	• The JPC recommends that the word non-government organisation be inserted in the definition of "data fiduciary" in re-numbered Claus 3(15) after the word "a company" and before "juristic entity" as NGOs play a significant role in data collection for various purposes in rural areas. (para 2.32)

	(*15*) "**data processor**" means any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary;	(***16***) **"data principal"** means the natural person to whom the personal data relates; (***17***) **"data processor"** means any person, including a State, a company, a non-government organisation, (***) juristic entity or any individual, who processes personal data on behalf of a data fiduciary;	• NGOs are also added to the definition of "data processor" in re-numbered Clause 3(17), since the JPC was of the view that NGOs also process data on behalf of data fiduciaries for various reasons, and should come within the ambit of the law (para 2.33) • The JPC observes that the Data Protection Officer mentioned under Clause 30 plays an important role in the implementation of this legislation, and therefore, the definition of "data protection officer" was included in Clause 3(18). (para 2.34)
	(*16*) "**de-identification**" means the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal; (*17*) "**disaster**" shall have the same meaning as assigned to it in clause (*d*) of section 2 of the Disaster Management Act, 2005; (*18*) "**financial data**" means any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history; (*19*) "**genetic data**" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the behavioural characteristics, physiology or the health of that natural person and which result, in particular, from	**(18) "data protection officer"** means an officer who shall be appointed by the significant data fiduciary under section 30; (***19***) **"de-identification"** means the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal; (***20***) **"disaster"** shall have the same meaning as assigned to it in clause (*d*) of section 2 of the Disaster Management Act, 2005; (***21***) **"financial data"** means any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history; (***22***) **"genetic data"** means personal data relating to the inherited or acquired genetic characteristics of a natural person which gives unique information about the behavioral characteristics, physiology or the health of	

	an analysis of a biological sample from the natural person in question; (*20*) "**harm**" includes— (*i*) bodily or mental injury; (*ii*) loss, distortion or theft of identity; (*iii*) financial loss or loss of property; (*iv*) loss of reputation or humiliation; (*v*) loss of employment; (*vi*) any discriminatory treatment; (*vii*) any subjection to blackmail or extortion; (*viii*) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal; (*ix*) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or (*x*) any observation or surveillance that is not reasonably expected by the data principal; (*21*) "**health data**" means the data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, data associating the data principal to the provision of specific health services; (*22*) "**intra-group schemes**" means the schemes approved by the Authority under clause (*a*) of sub-section (*1*) of section 34;	that natural person and which result**s**, in particular, from an analysis of a biological sample from the natural person in question; **(*23*)** "**harm**" includes— (*i*) bodily or mental injury; (*ii*) loss, distortion or theft of identity; (*iii*) financial loss or loss of property, (*iv*) loss of reputation or humiliation; (*v*) loss of employment; (*vi*) any discriminatory treatment; (*vii*) any subjection to blackmail or extortion; (*viii*) any denial or withdrawal of a service, benefit or good**s** resulting from an evaluative decision about the data principal; (*ix*) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; (***) (*x*) any observation or surveillance that is not reasonably expected by the data principal; (xi) psychological manipulation which impairs the autonomy of the individual; or (xii) such other harm as may be prescribed; **(*24*) "health data"** means the data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, data associated with the data principal to the provision of specific health services; **(*25*) "intra-group schemes"** means the schemes approved by the Authority under clause (*a*) of sub-section (*1*) of section 34;	• The JPC believes that the definition of "harm" in re-numbered Clause 3(23) needs to be widened to incorporate harms such as psychological manipulations which impairs the autonomy of a person. The JPC also feels that there may be more considerations to identify harms in the future owing to increased technological innovations and, therefore, an enabling sub-clause (xii) has been added, empowering the government to include other kinds of harms. (para 2.36) • The JPC recommends that renumbered Clause 3(26), which defines "in writing" and communication in electronic form should also

	(*23*) "**in writing**" includes any communication in electronic format as defined in clause (r) of sub-section (1) of section 2 of the Information Technology Act, 2000;	***(26)*** **"in writing"** includes any communication or information in electronic form (***) generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device (***);	include the word "information" after "communication" and should use the exact wording of the IT Act 2000 to define the electronic form (para 2.37)
	(*24*) "**journalistic purpose**" means any activity intended towards the dissemination through print, electronic or any other media of factual reports, analysis, opinions, views or documentaries regarding— (*i*) news, recent or current events; or (*ii*) any other information which the data fiduciary believes the public, or any significantly discernible class of the public, to have an interest in;	***(27)*** **"journalistic purpose"** means any activity intended towards the dissemination through print, electronic or any other media of factual reports, analysis, opinions, views or documentaries regarding— (*i*) news, recent or current events; or (*ii*) any other information which the data fiduciary believes the public, or any significantly discernible class of the public, to have an interest in;	• The JPC finds that although the words "non-personal data" and "non-personal data breach" have been used in multiple parts of the Bill, they have not been defined. (para 2.38)
		(28) "non-personal data" means the data other than personal data; **(29) "non-personal data breach"** means any unauthorized including accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to non-personal data that compromises the confidentiality, integrity or availability of such data;	
	(*25*) "**notification**" means a notification published in the Official Gazette and the expression "notify" shall be construed accordingly; (*26*) "**official identifier**" means any number, code, or other identifier, assigned to a data principal under a law made by Parliament or any State Legislature which may be used for the purpose of verifying the identity of a data principal; (*27*) "**person**" includes— (*i*) an individual, (*ii*) a Hindu undivided family, (*iii*) a company,	**(30)"notification"** means a notification published in the Official Gazette and the expressions "notify" and "notified" shall be construed accordingly; ***(31)*** **"official identifier"** means any number, code, or other identifier, assigned to a data principal under a law made by Parliament or any State Legislature which may be used for the purpose of verifying the identity of a data principal; ***(32)*** **"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 juridical person, not falling within any of the preceding sub-clauses; (*28*) "**personal data**" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling; (*29*) "**personal data breach**" means any unauthorised 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 to a data principal; (*30*) "**prescribed**" means prescribed by rules made under this Act; (*31*) "**processing**" in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction; (*32*) "**profiling**" means any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a data principal;	(*iv*) a firm; (*v*) an association of persons or a body of individuals, whether incorporated or not; (*vi*) the State; and (*vii*) every artificial juridical person, not falling within any of the preceding sub-clauses; **(*33*)** "**personal data"** means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling; **(*34*)** "**personal data breach"** means any unauthorised **(***)** including accidental disclosure, acquisition, sharing, use, alteration, destruction (***) or loss of access to personal data that compromises the confidentiality, integrity or availability of personal data to a data principal; **(*35*) "prescribed"** means prescribed by rules made under this Act; **(*36*) "processing"** in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction; **(*37*)** "**profiling"** means any form of processing of personal data that analyses or predicts aspects concerning the behavio**u**r, attributes or interests of a data principal;	

	(*33*) "**regulations**" means the regulations made by the Authority under this Act; (*34*) "**re-identification**" means the process by which a data fiduciary or data processor may reverse a process of de-identification; (*35*) "**Schedule**" means the Schedule appended to this Act; (*36*) "**sensitive personal data**" means such personal data, which may, reveal, be related to, or constitute— (*i*) financial data; (*ii*) health data; (*iii*) official identifier; (*iv*) sex life; (*v*) sexual orientation; (*vi*) biometric data; (*vii*) genetic data; (*viii*) transgender status; (*ix*) intersex status; (*x*) caste or tribe; (*xi*) religious or political belief or affiliation; or (*xii*) any other data categorised as sensitive personal data under section 15. *Explanation*.— For the purposes of this clause, the expressions,— (*a*) "**intersex status**" means the condition of a data principal who is— (*i*) a combination of female or male; (*ii*) neither wholly female nor wholly male; or (*iii*) neither female nor male; (*b*) "**transgender status**" means the condition of a data principal whose sense of gender does not match with the gender assigned to that data principal at birth, whether or not they have undergone sex reassignment surgery, hormone therapy, laser therapy, or any other similar medical procedure;	***(38)*** **"regulations"** means the regulations made by the Authority under this Act; ***(39)*** **"re-identification"** means the process by which a data fiduciary or data processor may reverse a process of de- identification; ***(40)*** **"Schedule"** means the Schedule appended to this Act; ***(41)*** **"sensitive personal data"** means such personal data, which may reveal, be related to, or constitute— (*i*) financial data; (*ii*) health data; (*iii*) official identifier; (*iv*) sex life; (*v*) sexual orientation; (*vi*) biometric data; (*vii*) genetic data; (*viii*) transgender status; (*ix*) intersex status; (*x*) caste or tribe; (*xi*) religious or political belief or affiliation; or (*xii*) any other data categorised as sensitive personal data under section 15; *Explanation*.— For the purposes of this clause, the expressions,— (*a*) "**intersex status**" means the condition of a data principal who is— (*i*) a combination of female or male; (*ii*) neither wholly female nor wholly male; or (*iii*) neither female nor male; (*b*) "**transgender status**" means the condition of a data principal whose sense of gender does not match with the gender assigned to that data principal at birth, whether or not they have undergone sex reassignment surgery, hormone therapy, laser therapy, or any other similar medical procedure;	

	(*37*) "**significant data fiduciary**" means a data fiduciary classified as such under sub-section (*1*) of section 26; (*38*) "**significant harm**" means harm that has an aggravated effect having regard to the nature of the personal data being processed, the impact, continuity, persistence or irreversibility of the harm; (*39*) "**State**" means the State as defined under article 12 of the Constitution; (*40*) "**systematic activity**" means any structured or organised activity that involves an element of planning, method, continuity or persistence.	(***42***) "**significant data fiduciary**" means a data fiduciary classified as such under sub-section (*1*) of section 26; (***43***) "**significant harm**" means harm that has an aggravated effect having regard to the nature of the personal data being processed, the impact, continuity, persistence or irreversibility of the harm; (***44***) **"social media platform"** means a platform which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services; (***45***) "**State**" means the State as defined under article 12 of the Constitution; (***46***) "**systematic activity**" means any structured or organised activity that involves an element of planning, method, continuity or persistence.	• The JPC notes that the term "social media intermediary" which is defined as an explanation to Clause 26(4) should be included in the definitions clause. The JPC also recommends that the more appropriate term would be "social media platform"- because social media intermediaries are currently functioning as internet based intermediaries as well as platforms where people communicate through various socialising applications and websites. (para 2.39). The JPC suggests retaining the definition from the Bill (changing intermediary to platform), but removes the exemptions for hosting services, search engines, and intermediaries that primarily enable commercial or business oriented transactions.
CHAPTER II: OBLIGATIONS OF DATA FIDUCIARIES			
6.	***Clause 4: Prohibition of processing of personal data.*** No personal data shall be processed by any person, except for any specific, clear and lawful purpose.	***Clause 4: Prohibition of processing of personal data.*** (***) The processing of personal data (***) by any person (***) shall be subject to the provisions of this Act and the rules and regulations made thereunder.	• The JPC acknowledges that it had received suggestions from experts and stakeholders that lawful, clear, and specific are not defined. The JPC finds that the language of the clause give a 'negative connotation', and therefore, recommends

			rewording it to make it more effective. (paras 2.40 and 2.41).
7.	***Clause 5: Limitation on purpose of processing of personal data.*** Every person processing personal data of a data principal shall process such personal data— (*a*) in a fair and reasonable manner and ensure the privacy of the data principal; and (*b*) for the purpose consented to by the data principal or which is incidental to or connected with such purpose, and which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected.	***Clause 5: Limitation on purpose of processing of personal data.*** Every person processing personal data of a data principal shall process such personal data— (a) in a fair and reasonable manner and ensure the privacy of the data principal; and (b) for the purpose consented to by the data principal or which is incidental thereto or connected with such purpose or which is for the purpose of processing of personal data under section 12, and which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected.	• The JPC finds that while Clause 5 deals with limitations on the purpose of processing of personal data, there was no mention of grounds for processing personal data without consent as given under Clause 12. The JPC recommends adding a reference to Clause 12 to include the grounds for processing personal data without consent and enable state agencies to function smoothly. (para 2.43)
8.	***Clause 6: Limitation on collection of personal data.*** The personal data shall be collected only to the extent that is necessary for the purposes of processing of such personal data	***Clause 6: Limitation on collection of personal data.*** The personal data shall be collected only to the extent that is necessary for the purposes of processing of such personal data.	• No change.
9.	***Clause 7: Requirement of notice for collection or processing of personal data.*** (*1*) Every data fiduciary shall give to the data principal a notice, at the time of collection of the personal data, or if the data is not collected from the data principal, as soon as reasonably practicable, containing the following information, namely:—	***Clause 7: Requirement of notice for collection or processing of personal data.*** (1) Every data fiduciary shall give to the data principal **(***)**, at the time of collection of the personal data, or if the data is not collected from the data principal, as soon as is reasonably practicable, a notice containing the following information, namely:—	• The JPC only suggests cosmetic changes to Clause 7(1). • In Clause 7(2), the JPC removes the reference to 'reasonable person', replacing it with individual. This is not a material change.

	(*a*) the purposes for which the personal data is to be processed; (*b*) the nature and categories of personal data being collected; (*c*) the identity and contact details of the data fiduciary and the contact details of the data protection officer, if applicable; (*d*) the right of the data principal to withdraw his consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent; (*e*) the basis for such processing, and the consequences of the failure to provide such personal data, if the processing of the personal data is based on the grounds specified in sections 12 to 14; (*f*) the source of such collection, if the personal data is not collected from the data principal; (*g*) the individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable; *(h)* information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable; (*i*) the period for which the personal data shall be retained in terms of section 9 or where such period is not known, the criteria for determining such period; (*j*) the existence of and procedure for the exercise of rights mentioned in Chapter V and any related contact details for the same; (*k*) the procedure for grievance redressal under section 32; (*l*) the existence of a right to file complaints to the Authority;	(a) the purposes for which the personal data is to be processed; (b) the nature and categories of personal data being collected; (c) the identity and contact details of the data fiduciary and the contact details of the data protection officer, if applicable; (d) the right of the data principal to withdraw his consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent; (e) the basis for such processing, and the consequences of the failure to provide such personal data, if the processing of the personal data is based on the grounds (***) provided in sections 12 to 14; (f) the source of such collection, if the personal data is not collected from the data principal; (g) the individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable; (h) the information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable; (i) the period for which the personal data shall be retained in terms of section 9 or where such period is not known, the criteria for determining such period; (j) the existence of and procedure for the exercise of rights mentioned in Chapter V and any related contact details for the same; (k) the procedure for grievance redressal under section 32; (l) the existence of a right to file complaints to the Authority;	• In Clause 7(3), the JPC recommends removing 'substantially'. Such that a notice need not be given when it would prejudice the purpose of processing for non-consensual State purposes, and the State authority need not demonstrate that that such prejudice is 'substantial'.

	(*m*) where applicable, any rating in the form of a data trust score that may be assigned to the data fiduciary under sub-section (*5*) of section 29; and (*n*) any other information as may be specified by the regulations. (*2*) The notice referred to in sub-section (*1*) shall be clear, concise and easily comprehensible to a reasonable person and in multiple languages where necessary and practicable. (*3*) The provisions of sub-section (*1*) shall not apply where such notice substantially prejudices the purpose of processing of personal data under section 12.	(m) where applicable, any rating in the form of a data trust score that may be assigned to the data fiduciary under sub-section (5) of section 29; and (n) any other information as may be specified by regulations. (2) The notice referred to in sub-section (1) shall be clear, concise and easily comprehensible to an (***) individual and in multiple languages (***) to the extent necessary and practicable. (3) The provisions of sub-section (1) shall not apply where such notice (***) prejudices the purpose of processing of personal data under section 12.	
10.	***Clause 8: Quality of personal data processed.*** (*1*) The data fiduciary shall take necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed. (*2*) While taking any steps under sub-section (*1*), the data fiduciary shall have regard to whether the personal data— (*a*) is likely to be used to make a decision about the data principal; (*b*) is likely to be disclosed to other individuals or entities including other data fiduciaries or processors; or (*c*) is kept in a form that distinguishes personal data based on facts from personal data based on opinions or personal assessments. (*3*) Where personal data is disclosed to any other individual or entity, including other data fiduciary or	***Clause 8: Quality of personal data processed.*** (1) The data fiduciary shall take necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed. (2) While taking any steps under sub-section (1), the data fiduciary shall have regard to whether the personal data— (a) is likely to be used to make a decision about the data principal; (b) is likely to be disclosed to other individuals or entities including other data fiduciaries or processors; or (c) is kept in a form that distinguishes personal data based on facts from personal data based on opinions or personal assessments.	• The JPC considers Clause 8 to be a protective clause that defines the mandate of the processing of personal data. Under Clause 8(3), if a DF has shared data with a third party, and finds such data to be incomplete/ misleading/ inaccurate, it was required to take 'reasonable steps' to notify the third party of this fact. The JPC recommends this should be mandatorily and taking 'reasonable steps' should not suffice. (para 2.46) • At the same time, the JPC believes this should not create hurdles in the smooth functioning of government agencies processing personal data. Therefore, a proviso to Clause 8(3) has been included to ensure that the functioning of the government agencies is not compromised, when the mandatory notice prejudices the processing of personal data under Section 12. (para 2.47)

	processor, and the data fiduciary finds that such data does not comply with the requirement of sub-section (*1*), the data fiduciary shall take reasonable steps to notify such individual or entity of this fact.	(3) Where personal data is disclosed to any other individual or entity, including other data fiduciary or processor, and the data fiduciary finds that such data does not comply with the requirements of sub-section (1), the data fiduciary shall (***) notify such individual or entity of this fact: Provided that the provisions of this sub-section shall not apply where such notice prejudices the purpose of processing of personal data under section 12. (4) A data fiduciary may share, transfer or transmit the personal data to any person as part of any business transaction in such manner as may be prescribed: Provided that the provisions of this sub-section shall not apply where such sharing, transfer or transmission of personal data prejudices the purpose of processing of personal data under Section 12.	• The JPC recommends a new sub-clause allowing DFs to share data with third parties as part of a business transaction, but in accordance with rules prescribed by the government. The JPC suggests this to 'curb' the seamless sharing, transfer, transmission of data under the garb of providing services. (para 2.48).
11.	***Clause 9: Restriction on retention of personal data.*** (1) The data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing. (2) Notwithstanding anything contained in sub-section (1), the personal data may be retained for a longer period if explicitly consented to by the data principal, or necessary to comply with any obligation under any law for the time being in force.	***Clause 9: Restriction on retention of personal data.*** (1) The data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of (***) such period. (2) Notwithstanding anything contained in sub-section (1), the personal data may be retained for a longer period if explicitly consented to by the data principal, or necessary to comply with any obligation under any law for the time being in force.	• The JPC believes that Clause 9(1) is very restrictive and may be a hurdle in the functioning of agencies which process data multiple times for various welfare purposes. Therefore, the JPC has recommended the deletion of the words "the processing" and its replacement with the words "such period". (para 2.50)

	(3) The data fiduciary shall undertake periodic review to determine whether it is necessary to retain the personal data in its possession. (4) Where it is not necessary for personal data to be retained by the data fiduciary under sub-section (1) or sub-section (2), then, such personal data shall be deleted in such manner as may be specified by regulations.	(3) The data fiduciary shall undertake periodic review to determine whether it is necessary to retain the personal data in its possession. (4) Where it is not necessary for personal data to be retained by the data fiduciary under sub-section (1) or sub-section (2), then, such personal data shall be deleted in such manner as may be specified by regulations.	
12.	***Clause 10. Accountability of data fiduciary.*** The data fiduciary shall be responsible for complying with the provisions of this Act in respect of any processing undertaken by it or on its behalf.	***Clause 10. Accountability of data fiduciary.*** The data fiduciary shall be responsible for complying with the provisions of this Act and the rules and regulations made thereunder in respect of any processing undertaken by it or on its behalf.	• The JPC suggests minor changes for clarity.
13.	***Clause 11: Consent necessary for processing of personal data.*** (*1*) The personal data shall not be processed, except on the consent given by the data principal at the commencement of its processing. (*2*) The consent of the data principal shall not be valid, unless such consent is— (*a*) free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872; (*b*) informed, having regard to whether the data principal has been provided with the information required under section 7;	***Clause 11: Consent necessary for processing of personal data*** (1) The personal data shall not be processed, except on the consent given by the data principal at the commencement of its processing. (2) The consent of the data principal shall not be valid, unless such consent is— (a) free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872; (b) informed, having regard to whether the data principal has been provided with the information required under section 7;	• The JPC observes that the language of Clause 11(3)(b) is ambiguous and needs clarity. Therefore, it recommended that the language of this clause must reflect the idea that the explicit consent of the data principal has to be obtained by specifying the conduct and context explicitly, without circumvention of law and without any kind of implicit inferences. This has been done by the insertion of the words "to be drawn either" after "inference" (para 2.54) • The JPC recommends that the scope of Clause 11(4) be extended to include denial based on exercise of choice. (para 2.55)

	(*c*) specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose of processing; (*d*) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and (*e*) capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given. (*3*) In addition to the provisions contained in sub-section (*2*), the consent of the data principal in respect of processing of any sensitive personal data shall be explicitly obtained— (*a*) after informing him the purpose of, or operation in, processing which is likely to cause significant harm to the data principal; (*b*) in clear terms without recourse to inference from conduct in a context; and (*c*) after giving him the choice of separately consenting to the purposes of, operations in, the use of different categories of, sensitive personal data relevant to processing. (*4*) The provision of any goods or services or the quality thereof, or the performance of any contract, or the enjoyment of any legal right or claim, shall not be made conditional on the consent to the processing of any personal data not necessary for that purpose. (*5*) The burden of proof that the consent has been given by the data principal for processing of the personal data under this section shall be on the data fiduciary.	(c)specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose of processing; (d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and (e) capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given. (3) In addition to the provisions contained in sub-section (2), the consent of the data principal in respect of processing of any sensitive personal data shall be explicitly obtained— (a) after informing him the purpose of, or operation in, processing which is likely to cause significant harm to the data principal; (b) in clear terms without recourse to inference to be drawn either from conduct (***) or context; and (c) after giving him the choice of separately consenting to the purposes of operations in the use of different categories of sensitive personal data relevant to processing. (4) The provision of any goods or services or the quality thereof, or the performance of any contract, or the enjoyment of any legal right or claim, shall not be,- (i) made conditional on the consent to the processing of any personal data not necessary for that purpose; and (ii) denied based on exercise of choice.	• The JPC recommends the deletion of the word “legal” from Clause 11(6). Such that the data principal is responsible for all consequences of withdrawal of consent, not just ‘legal’ consequences. (para 2.56)

	(*6*) Where the data principal withdraws his consent from the processing of any personal data without any valid reason, all legal consequences for the effects of such withdrawal shall be borne by such data principal.	(5) The burden of proof that the consent has been given by the data principal for processing of the personal data under this section shall be on the data fiduciary. (6) Where the data principal withdraws his consent from the processing of any personal data without any valid reason, (***) the consequences for the **(***)** same shall be borne by such data principal.	
CHAPTER III: GROUNDS FOR PROCESSING PERSONAL DATA WITHOUT CONSENT			
14.	***Clause 12: Grounds for processing of personal data without consent in certain cases.*** Notwithstanding anything contained in section 11, the personal data may be processed if such processing is necessary,— (a) for the performance of any function of the State authorised by law for— (i) the provision of any service or benefit to the data principal from the State; or (ii) the issuance of any certification, licence or permit for any action or activity of the data principal by the State; (b) under any law for the time being in force made by the Parliament or any State Legislature; or (c) for compliance with any order or judgment of any Court or Tribunal in India; (d) to respond to any medical emergency involving a threat to the life or a severe threat to the health of the data principal or any other individual;	***Clause 12: Grounds for processing of personal data without consent in certain cases.*** Notwithstanding anything contained in section 11, the personal data may be processed if such processing is necessary,— (a) for the performance of any function of the State authorised by law for— (i) the provision of any service or benefit to the data principal from the State; or (ii) the issuance of any certification, licence or permit for any action or activity of the data principal by the State; (b) under any law for the time being in force made by the Parliament or any State Legislature; or (c) for compliance with any order or judgment of any Court or Tribunal in India; (d) to respond to any medical emergency involving a threat to the life or a severe threat to the health of the data principal or any other individual;	• No change.

	(e) to undertake any measure to provide medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health; or (f) to undertake any measure to ensure safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order.	(e) to undertake any measure to provide medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health; or (f) to undertake any measure to ensure safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order.	
15.	***Clause 13: Processing of personal data necessary for purposes related to employment, etc.*** (1) Notwithstanding anything contained in section 11 and subject to sub-section (2), any personal data, not being any sensitive personal data, may be processed, if such processing is necessary for— (a) recruitment or termination of employment of a data principal by the data fiduciary; (b) provision of any service to, or benefit sought by, the data principal who is an employee of the data fiduciary; (c) verifying the attendance of the data principal who is an employee of the data fiduciary; or (d) any other activity relating to the assessment of the performance of the data principal who is an employee of the data fiduciary. (2) Any personal data, not being sensitive personal data, may be processed under sub-section (1), where the consent of the data principal is not appropriate having regard to the employment relationship between the data fiduciary and the data principal, or would involve a disproportionate effort on the part of the data	***Clause 13: Processing of personal data necessary for purposes related to employment, etc.*** (1) Notwithstanding anything contained in section 11 and subject to the provisions contained in sub-section (2), any personal data, not being any sensitive personal data, may be processed, if such processing is necessary or can reasonably be expected by the data principal for — (a) recruitment or termination of employment of a data principal by the data fiduciary; (b) provision of any service to, or benefit sought by, the data principal who is an employee of the data fiduciary; (c) verifying the attendance of the data principal who is an employee of the data fiduciary; or (d) any other activity relating to the assessment of the performance of the data principal who is an employee of the data fiduciary. (2) Any personal data, not being sensitive personal data, may be processed under sub-section (1), where the consent of the data principal is not appropriate having regard to the employment relationship between the data fiduciary and the data principal, or	• The JPC observes that in absence of employee's consent, the employer should not be given complete freedom to process their personal data. It takes note of the sensitive nature of the relationship between employer and employee. The JPC notes that an employee should be able to ensure that their personal data is not misused by their employers and is not processed for an unreasonable purpose. Accordingly, the JPC recommends that processing may happen if it is necessary or if it can "reasonably be expected by the data principal". (para 2.61) • The JPC does not extend the exception to processing of SPD like financial data, despite receiving suggestions to this effect. (para 2.58)

	fiduciary due to the nature of the processing under the said sub-section."	would involve a disproportionate effort on the part of the data fiduciary due to the nature of the processing under the said sub-section."	
16.	***Clause 14: Processing of personal data for other reasonable purposes.*** (1) In addition to the grounds referred to under sections 12 and 13, the personal data may be processed without obtaining consent under section 11, if such processing is necessary for such reasonable purposes as may be specified by regulations, after taking into consideration— (a) the interest of the data fiduciary in processing for that purpose; (b) whether the data fiduciary can reasonably be expected to obtain the consent of the data principal; (c) any public interest in processing for that purpose; (d) the effect of the processing activity on the rights of the data principal; and (e) the reasonable expectations of the data principal having regard to the context of the processing. (2) For the purpose of sub-section (1), the expression "reasonable purposes" may include— (a) prevention and detection of any unlawful activity including fraud;	***Clause 14: Processing of personal data for other reasonable purposes.*** (1) (***) Notwithstanding anything contained in section 11, the personal data may be processed (***), if such processing is necessary for (***) reasonable purposes as may be specified by regulations, after taking into consideration— (a) the legitimate interest of the data fiduciary in processing for that purpose; (b) whether the data fiduciary can reasonably be expected, and it is practicable to obtain the consent of the data principal; (c) any public interest in processing for that purpose; (d) the degree of any adverse effect of the processing activity on the rights of the data principal; and (e) the reasonable expectations of the data principal having regard to the context of the processing. (2) For the purpose of sub-section (1), the expression "reasonable purposes" may include—	• The JPC notes that this clause is an exception to clause 11, and suggests it should mirror the text of the other two exceptions (clauses 12 and 13) for clarity. So, it suggests beginning the clause with 'notwithstanding anything contained in Section 11". The JPC notes that this clause should not diminish the power of the Act with respect to other sectoral laws. (para 2.65) • The JPC does not accept suggestions to recognise contractual necessity as a ground for non-consensual processing or that DFs should be allowed to determine reasonable purposes, not the DPA through regulations. • Instead, the JPC opines that in absence of the data principal's consent, the principle of "legitimacy" would ensure accountability and would discourage any dilution of the law, by the data fiduciary. Hence, it recommends inserting the expression "legitimate" before "interest" in clause 14(1)(a). (para 2.65) • The JPC recommends inserting "and it is practicable" in clause 14(1)(b) and "degree of any adverse" in clause 14(1)(d), to balance the needs of the data fiduciary to process data vis-a-vis obtaining the data principal's consent. (para 2.65)

	(b) whistle blowing; (c) mergers and acquisitions; (d) network and information security; (e) credit scoring; (f) recovery of debt; (g) processing of publicly available personal data; and (h) the operation of search engines. (3) Where the Authority specifies a reasonable purpose under sub-section (1), it shall— (a) lay down, by regulations, such safeguards as may be appropriate to ensure the protection of the rights of data principals; and (b) determine where the provision of notice under section 7 shall apply or not apply having regard to the fact whether such provision shall substantially prejudice the relevant reasonable purpose.	(a) prevention and detection of any unlawful activity including fraud; (b) whistle blowing; (c) mergers (***), acquisitions, any other similar combination or corporate restructuring transactions in accordance with the provisions of applicable law ; (d) network and information security; (e) credit scoring; (f) recovery of debt; (g) processing of publicly available personal data; and (h) the operation of search engines. (3) Where the Authority specifies a reasonable purpose under sub-section (1), it shall— (a) lay down, by regulations, such safeguards as may be appropriate to ensure the protection of the rights of data principals; and (b) determine where the provision of notice under section 7 shall apply or not apply having regard to the fact whether such provision shall substantially prejudice the relevant reasonable purpose.	• Further, the JPC recommends inserting "any other similar combinations or corporate restructuring transactions in accordance with the provisions of applicable laws", in order to broaden the scope of clause 14(2)(c). (para 2.65)
17.	***Clause 15: Categorisation of personal data as sensitive personal data.*** (1) The Central Government shall, in consultation with the Authority and the sectoral regulator concerned, notify such categories of personal data as "sensitive personal data", having regard to—	***Clause 15: Categorisation of personal data as sensitive personal data.*** (1) The Central Government shall, in consultation with the Authority and the sectoral regulator concerned, notify such categories of personal data as "sensitive personal data", having regard to—	• No change.

	(a) the risk of significant harm that may be caused to the data principal by the processing of such category of personal data; (b) the expectation of confidentiality attached to such category of personal data; (c) whether a significantly discernible class of data principals may suffer significant harm from the processing of such category of personal data; and (d) the adequacy of protection afforded by ordinary provisions applicable to personal data. (2) The Authority may specify, by regulations, the additional safeguards or restrictions for the purposes of repeated, continuous or systematic collection of sensitive personal data for profiling of such personal data.	(a) the risk of significant harm that may be caused to the data principal by the processing of such category of personal data; (b) the expectation of confidentiality attached to such category of personal data; (c) whether a significantly discernible class of data principals may suffer significant harm from the processing of such category of personal data; and (d) the adequacy of protection afforded by ordinary provisions applicable to personal data. (2) The Authority may specify, by regulations, the additional safeguards or restrictions for the purposes of repeated, continuous or systematic collection of sensitive personal data for profiling of such personal data.	
CHAPTER IV: PERSONAL DATA (***) OF CHILDREN			
18.	***Chapter heading***: Personal data and sensitive personal data of children	***Chapter heading*** Personal data (***) of children	• The JPC recommends removing the expression "sensitive personal data" from the chapter heading, because there was no reference to the expression in the entire chapter (para 2.73)
19.	***Clause 16: Processing of personal data and sensitive personal data of children.*** (1) Every data fiduciary shall process personal data of a child in such manner that protects the rights of, and is in the best interests of, the child.	***Clause 16: Processing of personal data (***) of children.*** (1) Every data fiduciary shall process the personal data of a child in such manner that protects the rights of (***) the child.	• The JPC observes that qualifying phrases "in the best interests of the" the child may dilute the provisions and could give leeway for manipulation. So, it recommends deleting the expression "and is in the best interests of." in clause 16(1). (para 2.74)

	(2) The data fiduciary shall, before processing of any personal data of a child, verify his age and obtain the consent of his parent or guardian, in such manner as may be specified by regulations. (3) The manner for verification of the age of child under sub-section (2) shall be specified by regulations, taking into consideration— (a) the volume of personal data processed; (b) the proportion of such personal data likely to be that of child; (c) possibility of harm to child arising out of processing of personal data; and (d) such other factors as may be prescribed. (4) The Authority shall, by regulations, classify any data fiduciary, as guardian data fiduciary, who— (a) operate commercial websites or online services directed at children; or (b) process large volumes of personal data of children. (5) The guardian data fiduciary shall be barred from profiling, tracking or behavioural monitoring of, or targeted advertising directed at, children and undertaking any other processing of personal data that can cause significant harm to the child. (6) The provisions of sub-section (5) shall apply in such modified form to the data fiduciary offering counselling or child protection services to a child, as the Authority may, by regulations, specify. (7) A guardian data fiduciary providing exclusive counselling or child protection services to a child	(2) The data fiduciary shall, before processing of any personal data of a child, verify his age and obtain the consent of his parent or guardian, in such manner as may be specified by regulations. (3) The manner for verification of the age of child under sub-section (2) shall (***) take into consideration— (a) the volume of personal data processed; (b) the proportion of such personal data likely to be that of child; (c) the possibility of harm to child arising out of processing of personal data; and (d) such other factors as may be prescribed. (***) (4) The (***) data fiduciary shall be barred from profiling, tracking or behavioural monitoring of, or targeted advertising directed at, children and undertaking any other processing of personal data that can cause significant harm to the child. (5) The provisions of sub-section (4) shall apply in such modified form to the data fiduciary offering counselling or child protection services to a child, as the Authority may, by regulations, specify. (***) (***)	• The JPC observes that the consent of a guardian is sufficient to process a child's personal data. Further, given that both DFs and guardian fiduciaries have to comply with Clause 16, the JPC observes that a separate category of "guardian data fiduciary" does not offer any additional advantage. The JPC believes having two separate categories might lead to circumvention and dilution of the law. So, it recommends removing the concept of guardian DFs from the law. (para 2.75) • While earlier the bar on profiling/ tracking/ behaviourial monitoring was on guardian DFs only, now all DFs are barred from profiling, etc. (since the category of guardian DFs has been done away with). • The JPC observes the chapter does not require a DF to take a child's consent, once they attain the age of majority. (para 1.15.11.1) The JPC notes that this should be provided for in regulations framed by DPA. (para 1.15.11.2). The JPC recommends the following (to be brought in by regulations) (para 1.15.11.3) o Registration of data fiduciaries, exclusively dealing with children's data. o Application of the Majority Act to a contract with a child. o Obligation of Data fiduciary to inform a child to provide their consent, three months before such child attains majority.

	shall not require to obtain the consent of parent or guardian of the child under sub-section (2) Explanation.—For the purposes of this section, the expression "guardian data fiduciary" means any data fiduciary classified as a guardian data fiduciary under sub-section (4).		○ Continuation of the services until the child opts out or gives a fresh consent, upon achieving majority.
	CHAPTER V: RIGHTS OF DATA PRINCIPAL		
20.	***Clause 17: Right to Confirmation and Access:*** (1) The data principal shall have the right to obtain from the data fiduciary— (a) confirmation whether the data fiduciary is processing or has processed personal data of the data principal; (b) the personal data of the data principal being processed or that has been processed by the data fiduciary, or any summary thereof; (c) a brief summary of processing activities undertaken by the data fiduciary with respect to the personal data of the data principal, including any information provided in the notice under section 7 in relation to such processing (2) The data fiduciary shall provide the information under sub-section (1) to the data principal in a clear and concise manner that is easily comprehensible to a reasonable person. (3) The data principal shall have the right to access in one place the identities of the data fiduciaries with whom	***Clause 17: Right to Confirmation and Access:*** (1) The data principal shall have the right to obtain from the data fiduciary— (a) confirmation whether the data fiduciary is processing or has processed personal data of the data principal; (b) the personal data of the data principal being processed or that has been processed by the data fiduciary, or any summary thereof; (c) a brief summary of processing activities undertaken by the data fiduciary with respect to the personal data of the data principal, including any information provided in the notice under section 7 in relation to such processing (2) The data fiduciary shall provide the information under sub-section (1) to the data principal in a clear and concise manner that is easily comprehensible to a reasonable person. (3) The data principal shall have the right to access in one place the identities of the data fiduciaries with	• The JPC observes that the PDP Bill does not provide for the rights of a deceased data principle. Hence, it recommends adding a separate sub-clause (4) which allows the data principal to exercise certain rights and decide how their data shall be dealt with in the event of their death. (para 2.80)

	his personal data has been shared by any data fiduciary together with the categories of personal data shared with them, in such manner as may be specified by regulations.	whom his personal data has been shared by any data fiduciary together with the categories of personal data shared with them, in such manner as may be specified by regulations. (4) The data principal shall have the following options, namely:- (a) to nominate a legal heir or a legal representative as his nominee; (b) to exercise the right to be forgotten; and (c) to append the terms of agreement, with regard to processing of personal data in the event of the death of such data principal.	
21.	***Clause 18: Right to correction and erasure.*** (1) The data principal shall where necessary, having regard to the purposes for which personal data is being processed, subject to such conditions and in such manner as may be specified by regulations, have the right to— (a) the correction of inaccurate or misleading personal data; (b) the completion of incomplete personal data; (c) the updating of personal data that is out-of-date; and (d) the erasure of personal data which is no longer necessary for the purpose for which it was processed. (2) Where the data fiduciary receives a request under sub-section (1), and the data fiduciary does not agree with such correction, completion, updation or erasure having regard to the purposes of processing, such data	***Clause 18: Right to correction and erasure.*** (1) The data principal shall where necessary, having regard to the purposes for which personal data is being processed, subject to such conditions and in such manner as may be specified by regulations, have the right to— (a) the correction of inaccurate or misleading personal data; (b) the completion of incomplete personal data; (c) the updating of personal data that is out-of-date; and (d) the erasure of personal data which is no longer necessary for the purpose for which it was processed. (2) Where the data fiduciary receives a request under sub-section (1), and the data fiduciary does not agree with such correction, completion, updation or erasure having regard to the purposes of processing,	• No change. • Although it did not recommend any changes, the JPC did discuss the right to erasure. The JPC noted that it was limited only to cases where the personal data was no longer necessary for the purpose for which it was processed, and that did not provide an absolute right to seek erasure of data. (para 1.15.13.1) In this regard, the Ministry of Electronics and Information Technology (**MEITY**) deposed that the limitation had been added to prevent frivolous requests. (para 1.15.13.2). The MEITY also stated that the data principal had been provided sufficient safeguards under clause 18(2), 18(3) and 9(1). (para 1.15.13.6)

	fiduciary shall provide the data principal with adequate justification in writing for rejecting the application. (3) Where the data principal is not satisfied with the justification provided by the data fiduciary under sub-section (2), the data principal may require that the data fiduciary take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed by the data principal. (4) Where the data fiduciary corrects, completes, updates or erases any personal data in accordance with sub-section (1), such data fiduciary shall also take necessary steps to notify all relevant entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion, updation or erasure, particularly where such action may have an impact on the rights and interests of the data principal or on decisions made regarding them.	such data fiduciary shall provide the data principal with adequate justification in writing for rejecting the application. (3) Where the data principal is not satisfied with the justification provided by the data fiduciary under sub-section (2), the data principal may require that the data fiduciary take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed by the data principal. (4) Where the data fiduciary corrects, completes, updates or erases any personal data in accordance with sub-section (1), such data fiduciary shall also take necessary steps to notify all relevant entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion, updation or erasure, particularly where such action may have an impact on the rights and interests of the data principal or on decisions made regarding them.	
22.	***Clause 19: Right to data portability:*** (1) Where the processing has been carried out through automated means, the data principal shall have the right to— (a) receive the following personal data in a structured, commonly used and machine-readable format— (i) the personal data provided to the data fiduciary;	***Clause 19: Right to data portability:*** (1) Where the processing has been carried out through automated means, the data principal shall have the right to— (a) receive the following personal data in a structured, commonly used and machine-readable format— (i) the personal data provided to the data fiduciary;	• The JPC observes that Clause 19(2)(b) provides scope for data fiduciaries to conceal their actions by denying data portability under the garb of trade secrets or non-feasibility. (para 2.85) • Given the dynamic nature of the term "trade secrets" and its meaning in different domains, the JPC states that the term can't be defined under the PDP Bill and therefore recommends that the same cannot be a ground to deny data portability. (para 2.85)

	(ii) the data which has been generated in the course of provision of services or use of goods by the data fiduciary; or (iii) the data which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained; and (b) have the personal data referred to in Clause (a) transferred to any other data fiduciary in the format referred to in that Clause. (2) The provisions of sub-section (1) shall not apply where— (a) processing is necessary for functions of the State or in compliance of law or order of a court under section 12; (b) compliance with the request in sub-section (1) would reveal a trade secret of any data fiduciary or would not be technically feasible.	(ii) the data which has been generated in the course of provision of services or use of goods by the data fiduciary; or (iii) the data which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained; and (b) have the personal data referred to in Clause (a) transferred to any other data fiduciary in the format referred to in that Clause. (2) The provisions of sub-section (1) shall not apply where— (a) processing is necessary for functions of the State or in compliance (***) with any judgment or order of (***) any court, quasi-judicial authority or Tribunal under section 12; (b) compliance with the request in sub-section (1) would (***) not be technically feasible, as determined by the data fiduciary in such manner as may be specified by regulations.	• It also recommends that data portability should be denied only on the grounds of such technical feasibility, which has to be "strictly" determined by the regulations. (para 2.85)
23.	***Clause 20: Right to be forgotten.*** (1) The data principal shall have the right to restrict or prevent the continuing disclosure of his personal data by a data fiduciary where such disclosure— (a) has served the purpose for which it was collected or is no longer necessary for the purpose; (b) was made with the consent of the data principal under section 11 and such consent has since been withdrawn; or (c) was made contrary to the provisions of this Act or any other law for the time being in force.	***Clause 20: Right to be forgotten.*** (1) The data principal shall have the right to restrict or prevent the continuing disclosure or processing of his personal data by a data fiduciary where such disclosure or processing — (a) has served the purpose for which it was collected or is no longer necessary for the purpose; (b) was made with the consent of the data principal under section 11 and such consent has since been withdrawn; or	• The JPC notes that the expression 'disclosure' is insufficient. It observes that if the right to be forgotten is exercised, the data fiduciary might still "process" the data without "disclosing" it to third parties. Hence, the JPC recommends adding the word "processing" along with the word "disclosure" to make the clause comprehensive and meaningful. (para 2.90) • The JPC recommends clarifying that an individual must be able to show that her exercise of the right to be forgotten overrides

	(2) The rights under sub-section (1) may be enforced only on an order of the Adjudicating Officer made on an application filed by the data principal, in such form and manner as may be prescribed, on any of the grounds specified under clauses (a), (b) or clause (c) of that sub-section: Provided that no order shall be made under this sub-section unless it is shown by the data principal that his right or interest in preventing or restricting the continued disclosure of his personal data overrides the right to freedom of speech and expression and the right to information of any other citizen. (3) The Adjudicating Officer shall, while making an order under sub-section (2), having regard to— (a) the sensitivity of the personal data; (b) the scale of disclosure and the degree of accessibility sought to be restricted or prevented; (c) the role of the data principal in public life; (d) the relevance of the personal data to the public; and (e) the nature of the disclosure and of the activities of the data fiduciary, particularly whether the data fiduciary systematically facilitates access to personal data and whether the activities shall be significantly impeded if disclosures of the relevant nature were to be restricted or prevented. (4) Where any person finds that personal data, the disclosure of which has been restricted or prevented by an order of the Adjudicating Officer under sub-section (2), does not satisfy the conditions referred to	(c) was made contrary to the provisions of this Act or any other law for the time being in force. (2) The rights under sub-section (1) may be enforced only on an order of the Adjudicating Officer made on an application filed by the data principal, in such form and manner as may be prescribed, on any of the grounds specified under clauses (a), (b) or (***) (c) of that sub-section: Provided that no order shall be made under this sub-section unless it is shown by the data principal that his right or interest in preventing or restricting the continued disclosure or processing of his personal data overrides the right to freedom of speech and expression and the right to information of any other citizen or the right of the data fiduciary to retain, use and process such data in accordance with the provisions of this Act and the rules and regulations made thereunder. (3) The Adjudicating Officer shall, while making an order under sub-section (2), having regard to— (a) the sensitivity of the personal data; (b) the scale of disclosure or processing and the degree of accessibility sought to be restricted or prevented; (c) the role of the data principal in public life; (d) the relevance of the personal data to the public; and (e) the nature of the disclosure or processing and of the activities of the data fiduciary, particularly whether the data fiduciary systematically facilitates access to personal data and whether	the DF's right to retain, use and process such data in accordance with this law/ rules/ regulations. (para 2.90) This means the burden of proof of establishing this falls with an individual.

	in that sub-section, he may apply for the review of that order to the Adjudicating Officer in such manner as may be prescribed, and the Adjudicating Officer shall review his order. (5) Any person aggrieved by an order made under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal.	the activities shall be significantly impeded if disclosures or processing of the relevant nature were to be restricted or prevented. (4) Where any person finds that personal data, the disclosure or processing of which has been restricted or prevented by an order of the Adjudicating Officer under sub-section (2), does not satisfy the conditions referred to in that sub-section any longer, he may apply for the review of that order to the Adjudicating Officer in such manner as may be prescribed, and the Adjudicating Officer shall review his order. (5) Any person aggrieved by an order made under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal under section 73.	
24.	***Clause 21: General conditions for the exercise of rights in this Chapter:*** (1) The data principal, for exercising any right under this Chapter, except the right under section 20, shall make a request in writing to the data fiduciary either directly or through a consent manager with the necessary information as regard to his identity, and the data fiduciary shall acknowledge the receipt of such request within such period as may be specified by regulations. (2) For complying with the request made under sub-section (1), the data fiduciary may charge such fee as may be specified by regulations: Provided that no fee shall be required for any request in respect of rights	***Clause 21: General conditions for the exercise of rights in this Chapter:*** (1) The data principal, for exercising any right under this Chapter, except the right under section 20, shall make a request in writing to the data fiduciary either directly or through a consent manager with the necessary information as regard to his identity, and the data fiduciary shall acknowledge the receipt of such request within such period as may be specified by regulations. (2) For complying with the request made under sub-section (1), the data fiduciary may charge such fee as may be specified by regulations: Provided that no fee shall be required for any request in respect of	• The JPC notes that sub-clause (5) provides arbitrary powers to DFs to reject a data principal's request- on the ground that it harms the rights of another individual. To prevent unnecessary refusal of requests, it recommends adding a proviso empowering the DPA to make regulations to determine the rationale behind a denial of the data principal's request. (para 2.93)

	referred to in clause (a) or (b) of sub-section (1) of section 17 or section 18. (3) The data fiduciary shall comply with the request under this Chapter and communicate the same to the data principal, within such period as may be specified by regulations. (4) Where any request made under this Chapter is refused by the data fiduciary, it shall provide the data principal the reasons in writing for such refusal and shall inform the data principal regarding the right to file a complaint with the Authority against the refusal, within such period and in such manner as may be specified by regulations. (5) The data fiduciary is not obliged to comply with any request under this Chapter where such compliance shall harm the rights of any other data principal under this Act.	rights referred to in clause (a) or (b) of sub-section (1) of section 17 or section 18. (3) The data fiduciary shall comply with the request under this Chapter and communicate the same to the data principal, within such period as may be specified by regulations. (4) Where any request made under this Chapter is refused by the data fiduciary, it shall provide the data principal the reasons in writing for such refusal and shall inform the data principal regarding the right to file a complaint with the Authority against the refusal, within such period and in such manner as may be specified by regulations. (5) The data fiduciary is not obliged to comply with any request under this Chapter where such compliance shall harm the rights of any other data principal under this Act Provided that the data fiduciary shall, subject to such conditions as may be specified by regulations, be obliged to comply with such request made by the data principal.	
CHAPTER VI: TRANSPARENCY AND ACCOUNTABILITY MEASURES			
25.	***Clause 22: Privacy by design policy*** (1) Every data fiduciary shall prepare a privacy by design policy, containing—	***Clause 22: Privacy by design policy*** (1) Every data fiduciary shall prepare a privacy by design policy, containing—	• The JPC observes that the certification of the privacy by design policy should not hamper the growth of MSMEs. It suggests tweaking sub-clause (3) to allow the DPA to make regulations to exempt DFs below a

	(a) the managerial, organisational, business practices and technical systems designed to anticipate, identify and avoid harm to the data principal; *(b)* the obligations of data fiduciaries; *(c)* the technology used in the processing of personal data is in accordance with commercially accepted or certified standards; *(d)* the legitimate interests of businesses including any innovation is achieved without compromising privacy interests; *(e)* the protection of privacy throughout processing from the point of collection to deletion of personal data; *(f)* the processing of personal data in a transparent manner; and *(g)* the interest of the data principal is accounted for (2) Subject to the regulations made by the Authority, the data fiduciary may submit its privacy by design policy prepared under sub-section (1) to the Authority for certification within such period and in such manner as may be specified by regulations. (3) The Authority, or an officer authorised by it, shall certify the privacy by design policy on being satisfied that it complies with the requirements of sub-section (1). (4) The privacy by design policy certified under sub-section (3) shall be published on the website of the data fiduciary and the Authority	*(a)* the managerial, organisational, business practices and technical systems designed to anticipate, identify and avoid harm to the data principal; *(b)* the obligations of data fiduciaries; *(c)* the technology used in the processing of personal data is in accordance with commercially accepted or certified standards; *(d)* the legitimate interests of businesses including any innovation is achieved without compromising privacy interests; *(e)* the protection of privacy throughout processing from the point of collection to deletion of personal data; *(f)* the processing of personal data in a transparent manner; and *(g)* the interest of the data principal is accounted for (2) **(***)**The data fiduciary may submit its privacy by design policy prepared under sub-section (1) to the Authority for certification within such period and in such manner as may be specified by regulations. (3) Subject to the provisions contained in sub-section (2), the Authority, or an officer authorised by it, shall certify the privacy by design policy on being satisfied that it complies with the requirements of sub-section (1). (4) The privacy by design policy certified under sub-section (3) shall be published on the website of the data fiduciary and the Authority.	certain threshold from submitting a privacy by design policy. (para 2.96)
26.	***Clause 23: Transparency in processing of personal data***	***Clause 23: Transparency in processing of personal data***	• In its general recommendations, the JPC report briefly discusses GDPR's position on

	(1) Every data fiduciary shall take necessary steps to maintain transparency in processing personal data and shall make the following information available in such form and manner as may be specified by regulations— *(a)* the categories of personal data generally collected and the manner of such collection; *(b)* the purposes for which personal data is generally processed; *(c)* any categories of personal data processed in exceptional situations or any exceptional purposes of processing that create a risk of significant harm; *(d)* the existence of and the procedure for exercise of rights of data principal under Chapter V and any related contact details for the same; *(e)* the right of data principal to file complaint against the data fiduciary to the Authority; *(f)* where applicable, any rating in the form of a data trust score that may be accorded to the data fiduciary under sub-section (5) of section 29; *(g)* where applicable, information regarding cross-border transfers of personal data that the data fiduciary generally carries out and; *(h)* any other information as may be specified by regulations. (2) The data fiduciary shall notify, from time to time, the important operations in the processing of personal data related to the data principal in such manner as may be specified by regulations. (3) The data principal may give or withdraw his consent to the data fiduciary through a Consent Manager.	(1) Every data fiduciary shall take necessary steps to maintain transparency in processing personal data and shall make the following information available in such form and manner as may be specified by regulations— *(a)* the categories of personal data generally collected and the manner of such collection; *(b)* the purposes for which personal data is generally processed; *(c)* any categories of personal data processed in exceptional situations or any exceptional purposes of processing that create a risk of significant harm; *(d)* the existence of and the procedure for exercise of rights of data principal under Chapter V and any related contact details for the same; *(e)* the right of data principal to file complaint against the data fiduciary to the Authority; *(f)* where applicable, any rating in the form of a data trust score that may be accorded to the data fiduciary under sub-section (5) of section 29; *(g)* where applicable, information regarding cross-border transfers of personal data that the data fiduciary generally carries out; (***) *(h)* where applicable, fairness of algorithm or method used for processing of personal data; and *(i)* any other information as may be specified by regulations. (2) The data fiduciary shall notify, from time to time, the important operations in the processing of personal data related to the data principal in such manner as may be specified by regulations.	automated data making and how algorithms profile, aggregate and make predictions on the basis of user data, without their consent. It notes that the GDPR allows citizens to keep their data 'out of automated decision making' which has legal or other impact. (para 1.13.3) • While the JPC does not introduce the right of an individual to object to automated decision-making, it recommends that DFs must disclose the fairness of algorithms and methods used for processing- to ensure transparency of algorithms used for processing personal data and to prevent its misuse. (para 2.99). • The JPC removes the definition of "consent manager" from the clause since it has been defined in the definitions clause. (para 2.100)

	(4) Where the data principal gives or withdraws consent to the data fiduciary through a Consent Manager, such consent or its withdrawal shall be deemed to have been communicated directly by the data principal. (5) The consent manager under sub-section (3), shall be registered with the Authority in such manner and subject to such technical, operational, financial and other conditions as may be specified by regulations. *Explanation.*- For the purposes of this section, a "consent manager" is a data fiduciary which enables a data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platform	(3) The data principal may give or withdraw his consent to the data fiduciary through a Consent Manager. (4) Where the data principal gives or withdraws consent to the data fiduciary through a Consent Manager, such consent or its withdrawal shall be deemed to have been communicated directly by the data principal. (5) The Consent Manager under sub-section (3), shall be registered with the Authority in such manner and subject to such technical, operational, financial and other conditions as may be specified by regulations. *Explanation.*-(***)	
27.	***Clause 24: Security Safeguards*** (1) Every data fiduciary and the data processor shall, having regard to the nature, scope and purpose of processing personal data, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, implement necessary security safeguards, including— *(a)* use of methods such as de-identification and encryption; *(b)* steps necessary to protect the integrity of personal data; and *(c)* steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.	***Clause 24: Security Safeguards*** (1) Every data fiduciary and the data processor shall, having regard to the nature, scope and purpose of processing personal data, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, implement necessary security safeguards, including— *(a)* use of methods such as de-identification and encryption; *(b)* steps necessary to protect the integrity of personal data; and *(c)* steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.	• No change.

	(2) Every data fiduciary and data processor shall undertake a review of its security safeguards periodically in such manner as may be specified by regulations and take appropriate measures accordingly.	(2) Every data fiduciary and data processor shall undertake a review of its security safeguards periodically in such manner as may be specified by regulations and take appropriate measures accordingly.	
28.	***Clause 25: Reporting of personal data breach*** (1) Every data fiduciary shall by notice inform the Authority about the breach of any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal. (2) The notice referred to in sub-section (1) shall include the following particulars, namely:— *(a)* nature of personal data which is the subject matter of the breach; *(b)* number of data principals affected by the breach; *(c)* possible consequences of the breach; and *(d)* action being taken by the data fiduciary to remedy the breach. (3) The notice referred to in sub-section (1) shall be made by the data fiduciary to the Authority as soon as possible and within such period as may be specified by regulations, following the breach after accounting for any period that may be required to adopt any urgent measures to remedy the breach or mitigate any immediate harm. (4) Where it is not possible to provide all the information specified in sub-section (2) at the same time, the data fiduciary shall provide such	***Clause 25: Reporting of (***) Breach*** (1) Every data fiduciary shall by notice, (***) report to the Authority about the breach of any personal data processed by (***) such data fiduciary.**(***)** (2) The notice referred to in sub-section (1) shall be in such form as may be specified by regulations and include the following particulars, namely:— *(a)* nature of personal data which is the subject matter of the breach; *(b)* number of data principals affected by (***) such breach; *(c)* possible consequences of (***) such breach; and *(d)* the remedial actions being taken by the data fiduciary (***) for such breach. (3) The notice referred to in sub-section (1) shall be (***) issued by the data fiduciary within seventy-two hours of becoming aware of such breach.(***) (4) Where it is not possible to provide all the information (***) provided in sub-section (2) at the same time, the data fiduciary shall provide such information to the Authority in phases without any undue delay.	• The JPC amends the marginal heading of Clause 25 to include both personal and non-personal data. (para 2.107) • Significantly, the JPC recommends that the DPA be empowered to take necessary steps in the event of breach of non-personal data. This will be further prescribed by rules made by the government. • Instead of breaches that are likely to cause harm, the JPC recommends that DFs must report all personal data breaches to the DPA. This is because the reference to harm could lead to ambiguity. (paras 2.102-2.105, 2.108) • The form of reporting the data breach shall now be prescribed through regulations, rather than restricting the scope of the form within the law itself, and the JPC makes language changes to the Bill text to clarify this. Clause 25(2)(d) is amended to clarify that the notice must include particulars of the remedial actions taken by the data fiduciary for incidents of data breach. (para 2.109, 2.110) • The JPC recommends a 72-hour limit for reporting personal data breaches (starting

	information to the Authority in phases without undue delay. (5) Upon receipt of a notice, the Authority shall determine whether such breach should be reported by the data fiduciary to the data principal, taking into account the severity of the harm that may be caused to such data principal or whether some action is required on the part of the data principal to mitigate such harm. (6) The Authority may, in addition to requiring the data fiduciary to report the personal data breach to the data principal under sub-section (5), direct the data fiduciary to take appropriate remedial action as soon as possible and to conspicuously post the details of the personal data breach on its website. (7) The Authority may, in addition, also post the details of the personal data breach on its website.	**(5) (***)** (5) The Authority (***)shall, after taking into account the personal data breach and the severity of harm that may be caused to the data principal, direct the data fiduciary to report such breach to the data principal and take appropriate remedial actions(***) to mitigate such harm and to conspicuously post the details of the personal data breach on its website. Provided that the Authority may direct the data fiduciary to adopt any urgent measures to remedy such breach or mitigate any harm caused to the data principal. **(7)(***)** (6) The Authority shall, in case of breach of non-personal data, take such necessary steps as may be prescribed.	from the time the data fiduciary has become aware of the breach). (para 2.111) • The JPC notes that "it is not advisable" to report all kinds of data breaches to data principals since the disclosure of all data breach incidents could lead to panic among users or affect public law and order. So, it does not add a requirement to notify individuals directly about all breaches, but retains the earlier position- that DFs must report breaches to the DPA, and the DPA decides whether the breach should be reported to individuals. (para 2.112)
29.	***Clause 26: Classification of data fiduciaries as significant data fiduciaries*** (1) The Authority shall, having regard to the **any of the** following factors, notify any data fiduciary or class of data fiduciary as significant data fiduciary, namely:— *(a)* volume of personal data processed; *(b)* sensitivity of personal data processed; *(c)* turnover of the data fiduciary; *(d)* risk of harm by processing by the data fiduciary; *(e)* use of new technologies for processing; *(f)* any other factor causing harm from such processing.	***Clause 26: Classification of data fiduciaries as significant data fiduciaries*** (1) The Authority shall, having regard to the any of the following factors, notify any data fiduciary or class of data fiduciary as significant data fiduciary, namely:— *(a)* volume of personal data processed; *(b)* sensitivity of personal data processed; *(c)* turnover of the data fiduciary; *(d)* risk of harm by processing by the data fiduciary; *(e)* use of new technologies for processing; (***) *(f)* any social media platform-	• The JPC extensively discusses the role of social media intermediaries (that they act "as if they are above the sovereign"). According to the JPC, most social media intermediaries are actually working as internet-based intermediaries and platforms, where people communicate through various socializing apps and websites. The JPC recommends that the term social media 'intermediary' should be replaced with "social media platforms" (para 2.117). The provisions of Clause 26(1)(f) have been modified to include social media platforms (above a certain user threshold and whose actions can significantly

	(2) The data fiduciary or class of data fiduciary referred to in sub-section (1) shall register itself with the Authority in such manner as may be specified by regulations. (3) Notwithstanding anything in this Act, if the Authority is of the opinion that any processing by any data fiduciary or class of data fiduciary carries a risk of significant harm to any data principal, it may, by notification, apply all or any of the obligations specified in sections 27 to 30 to such data fiduciary or class of data fiduciary as if it is a significant data fiduciary. (4) Notwithstanding anything contained in this section, any social media intermediary,— (i) with users above such threshold as may be notified by the Central Government, in consultation with the Authority; and (ii) whose actions have, or are likely to have a significant impact on electoral democracy, security of the State, public order or the sovereignty and integrity of shall be notified by the Central Government, in consultation with the Authority, as a significant data fiduciary: Provided that different thresholds may be notified for different classes of social media intermediaries. Explanation.—For the purposes of this sub-section, a "social media intermediary" is an intermediary who primarily or solely enables online	(iii) with users above such threshold as may be prescribed, in consultation with the Authority; and (iv) whose actions have or are likely to have a significant impact on the sovereignty and integrity of India, electoral democracy, security of the State or public order: Provided that different thresholds may be prescribed for different classes of social media platforms; *(g)* the processing of data relating to children or provision of services to them; or *(h)* any other factor causing harm from such processing. (2) The data fiduciary or class of data fiduciary referred to in sub-section (1) shall register itself with the Authority in such manner as may be specified by regulations. (3) Notwithstanding anything contained in this Act, if the Authority is (***) satisfied that any processing by any data fiduciary or class of data fiduciar**ies** carries a risk of significant harm to any data principal, it may, by notification, apply all or any of the obligations (***)provided in sections 27 to 30 to such data fiduciary or class of data fiduciaries, as if it is a significant data fiduciary. **(4) (***)** (4) Subject to the provisions contained in section 56, the significant data fiduciary shall be regulated by such regulations as may be made by the respective sectoral regulators.	impact sovereignty, etc. of India) as one of the factors for classification of DFs as significant DFs. (para 2.118) • In the JPC's view, SDFs need to be transparent and accountable. So, it recommends the insertion of Clause 26(4) such that SDFs will be regulated by the sectoral regulators. (para 2.121) • The JPC also discusses the urgent need to curb the misuse of children's data, which compromises the data of their parents also. So, it recommends that processing of children's data or providing services to children should be a factor for classification as an to SDF. (para 2.119)

	interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services, but shall not include intermediaries which primarily, - *(a)* enable commercial or business oriented transactions; *(b)* provide access to the Internet; *(c)* in the nature of search-engines, on-line encyclopedias, e-mail services or on-line storage services.		
30.	***Clause 27: Data protection impact assessment*** (1) Where the significant data fiduciary intends to undertake any processing involving new technologies or large scale profiling or use of sensitive personal data such as genetic data or biometric data, or any other processing which carries a risk of significant harm to data principals, such processing shall not be commenced unless the data fiduciary has undertaken a data protection impact assessment in accordance with the provisions of this section. (2) The Authority may by regulations specify, such circumstances or class of data fiduciary or processing operation where such data protection impact assessment shall be mandatory, and also specify the instances where a data auditor under this Act shall be engaged by the data fiduciary to undertake a data protection impact assessment. (3) A data protection impact assessment shall, inter alia, contain—	***Clause 27: Data protection impact assessment*** (1) Where (***) a significant data fiduciary intends to undertake any processing involving new technologies or large scale profiling or use of sensitive personal data such as genetic data or biometric data, or any other processing which carries a risk of significant harm to data principals, such processing shall not be commenced unless the data fiduciary has undertaken a data protection impact assessment in accordance with the provisions of this section. (2) The Authority may by regulations specify, such circumstances or class of data fiduciar**ies** or processing operation where such data protection impact assessment shall be mandatory, and also specify the instances where a data auditor under this Act shall be engaged by the data fiduciary to undertake a data protection impact assessment. (3) A data protection impact assessment shall, *inter alia*, contain—	• The JPC recommends only cosmetic changes.

	(a) detailed description of the proposed processing operation, the purpose of processing and the nature of personal data being processed; *(b)* assessment of the potential harm that may be caused to the data principals whose personal data is proposed to be processed; and *(c)* measures for managing, minimising, mitigating or removing such risk of harm. (4) Upon completion of the data protection impact assessment, the data protection officer appointed under sub-section (1) of section 30, shall review the assessment and submit the assessment with his finding to the Authority in such manner as may be specified by regulations. (5) On receipt of the assessment and its review, if the Authority has reason to believe that the processing is likely to cause harm to the data principals, the Authority may direct the data fiduciary to cease such processing or direct that such processing shall be subject to such conditions as the Authority may deem fit.	*(a)* detailed description of the proposed processing operation, the purpose of processing and the nature of personal data being processed; *(b)* assessment of the potential harm that may be caused to the data principals whose personal data is proposed to be processed; and *(c)* measures for managing, minimising, mitigating or removing such risk of harm. (4) Upon completion of the data protection impact assessment, the data protection officer appointed under sub-section (1) of section 30, shall review the assessment and submit the assessment with his finding to the Authority in such manner as may be specified by regulations. (5) On receipt of the assessment and its review, if the Authority has (***) satisfied itself that the processing is likely to cause harm to the data principals, (***) it may direct the data fiduciary to cease such processing or direct that such processing shall be subject to such conditions as (***) may be specified by regulations.	
31.	***Clause 28: Maintenance of records*** (1) The significant data fiduciary shall maintain accurate and up-to-date records of the following, in such form and manner as may be specified by regulations, namely:— *(a)* important operations in the data life-cycle including collection, transfers, and erasure of personal data to demonstrate compliance as required under section 10;	***Clause 28: Maintenance of records*** (1) The significant data fiduciary shall maintain accurate and up-to-date records of the following, in such form and manner as may be specified by regulations, namely:— *(d)* important operations in the data life-cycle including collection, transfers, and erasure of personal data to demonstrate compliance as required under section 10;	• While it does not make any changes to the Bill, the JPC notes that social media platforms must verify accounts. And that a mechanism should be devised such that social media platforms which are not acting as intermediaries, are liable for content hosted by unverified accounts. The JPC does note that this law is about personal data protection and that social media regulation needs separate, detailed deliberation. (para 2.126 and 1.15.12.7)

	(b) periodic review of security safeguards under section 24; *(c)* data protection impact assessments under section 27; and *(d)* any other aspect of processing as may be specified by regulations. (2) Notwithstanding anything contained in this Act, this section shall also apply to the State. (3) Every social media intermediary which is notified as a significant data fiduciary under sub-section (4) of section 26 shall enable the users who register their service from India, or use their services in India, to voluntarily verify their accounts in such manner as may be prescribed. *(4)* Any user who voluntarily verifies his account shall be provided with such demonstrable and visible mark of verification, which shall be visible to all users of the service, in such manner as may be prescribed.	*(e)* periodic review of security safeguards under section 24; *(f)* data protection impact assessments under section 27; and *(g)* any other aspect of processing as may be specified by regulations. (2) Notwithstanding anything contained in this Act, this section shall also apply to the State. (3) Every social media (***) platform which is notified as a significant data fiduciary under sub-section (***) (1) of section 26 shall enable the (***) persons who register their service from India, or use their services in India, to voluntarily verify their accounts in such manner as may be prescribed. *(4)* Any (***) person who voluntarily verifies his account on a social media platform referred to in sub-section (3) shall be provided with such demonstrable and visible mark of verification, which shall be visible to all users of the service, in such manner as may be prescribed.	
32.	***Clause 29: Audit of policies and conduct of processing etc.*** (1) The significant data fiduciary shall have its policies and the conduct of its processing of personal data audited annually by an independent data auditor under this Act. (2) The data auditor shall evaluate the compliance of the data fiduciary with the provisions of this Act, including—	***Clause 29: Audit of policies and conduct of processing etc.*** (1) The significant data fiduciary shall have its policies and the conduct of its processing of personal data audited annually by an independent data auditor under this Act. (2) The data auditor shall evaluate the compliance of the data fiduciary with the provisions of this Act, including—	• The JPC recommends that the DPA should encourage concurrent audits. (para 2.131)

	(a) clarity and effectiveness of notices under section 7; *(b)* effectiveness of measures adopted under section 22; *(c)* transparency in relation to processing activities under section 23; *(d)* security safeguards adopted pursuant to section 24; *(e)* instances of personal data breach and response of the data fiduciary, including the promptness of notice to the Authority under section 25; *(f)* timely implementation of processes and effective adherence to obligations under sub-section (3) of section 28; and *(g)* any other matter as may be specified by regulations. (3) The Authority shall specify, by regulations, the form and procedure for conducting audits under this section. (4) The Authority shall register in such manner, the persons with expertise in the area of information technology, computer systems, data science, data protection or privacy, possessing such qualifications, experience and eligibility having regard to factors such as independence, integrity and ability, as it may be specified by regulations, as data auditors under this Act. (5) A data auditor may assign a rating in the form of a data trust score to the data fiduciary pursuant to a data audit conducted under this section. (6) The Authority shall, by regulations, specify the criteria for assigning a rating in the form of a data trust	*(a)* clarity and effectiveness of notices under section 7; *(b)* effectiveness of measures adopted under section 22; *(c)* transparency in relation to processing activities under section 23; *(d)* security safeguards adopted pursuant to section 24; *(e)* instances of personal data breach and response of the data fiduciary, including the promptness of notice to the Authority under section 25; *(f)* timely implementation of processes and effective adherence to obligations under sub-section (3) of section 28; and *(g)* any other matter as may be specified by regulations. (3) The Authority shall specify, by regulations, the form and procedure for conducting audits under this section and shall encourage the practice of appropriate concurrent audits. (4) The Authority shall register in such manner the persons, with expertise in the area of information technology, computer systems, data science, data protection or privacy, possessing such qualifications, experience and eligibility having regard to factors such as independence, integrity and ability, as (***) may be **(***)** prescribed, as data auditors (***). (5) A data auditor may assign a rating in the form of a data trust score to the data fiduciary pursuant to a data audit conducted under this section.	

	score having regard to the factors mentioned in sub-section (2). (7) Notwithstanding anything contained in sub-section (1), where the Authority is of the view that the data fiduciary is processing personal data in such manner that is likely to cause harm to a data principal, the Authority may direct the data fiduciary to conduct an audit and shall appoint a data auditor for that purpose	(6) The Authority shall, by regulations, specify the criteria for assigning a rating in the form of a data trust score having regard to the factors mentioned in sub-section (2). (7) Notwithstanding anything contained in sub-section (1), where the Authority is (***) satisfied that the data fiduciary is processing personal data in such manner that is likely to cause harm to a data principal, the Authority may direct (***) such data fiduciary to conduct an audit and shall appoint a data auditor for that purpose.	
33.	***Clause 30: Data Protection Officer*** (1) Every significant data fiduciary shall appoint a data protection officer possessing such qualification and experience as may be specified by regulations for carrying out the following functions:— *(a)* providing information and advice to the data fiduciary on matters relating to fulfilling its obligations under this Act; *(b)* monitoring personal data processing activities of the data fiduciary to ensure that such processing does not violate the provisions of this Act; *(c)* providing advice to the data fiduciary on carrying out the data protection impact assessments, and carry out its review under sub-section (4) of section 27; *(d)* providing advice to the data fiduciary on the development of internal mechanisms to satisfy the principles specified under section 22;	***Clause 30: Data Protection Officer*** (1) Every significant data fiduciary shall appoint a data protection officer who shall be a senior level officer in the State or a key managerial personnel in relation to a company or such other employee of equivalent capacity in case of other entities, as the case may be, possessing such qualifications and experience as may be (***) prescribed (***) for carrying out the following functions, namely:— *(a)* providing information and advice to the data fiduciary on matters relating to fulfilling its obligations under this Act; *(b)* monitoring personal data processing activities of the data fiduciary to ensure that such processing does not violate the provisions of this Act; *(c)* (***)providing assistance to and co-operating with the Authority on matters of compliance of the data fiduciary with the provisions under this Act;	• The JPC recommends that the data protection officer (DPO) should be a senior level officer in the State/ a key managerial personnel in a company/ employee of equivalent capacity for other entities. The JPC believes that the DPO plays a vital role and must hold an important position in the enterprise. • Key managerial personnel is defined as CEO or MD or manager, whole time director, CFO, Company Secretary, or other personnel prescribed by the government through rules. (para 2.137)

	(e) providing assistance to and co-operating with the Authority on matters of compliance of the data fiduciary with the provisions under this Act; *(f)* act as the point of contact for the data principal for the purpose of grievances redressal under section 32; and *(g)* maintaining an inventory of records to be maintained by the data fiduciary under section 28. (2) Nothing contained in sub-section (1) shall prevent the data fiduciary from assigning any other function to the data protection officer, which it may consider necessary. *(3)* The data protection officer appointed under sub-section (1) shall be based in India and shall represent the data fiduciary under this Act.	*(d)* providing advice to the data fiduciary on the development of internal mechanisms to satisfy the principles specified under section 22; *(e)* (***)providing advice to the data fiduciary on carrying out the data protection impact assessments, and carry out its review under sub-section (4) of section 27; *(f)* (***) maintaining an inventory of records to be maintained by the data fiduciary under section 28;and *(g)* (***) act as the point of contact for the data principal for the purpose of grievance (***) redressal under section 32. *Explanation*.- For the purposes of this sub-section, the expression "key managerial personnel" means— (i) the Chief Executive Officer or the managing director or the manager; (ii) the company secretary; (iii) the whole-time director; (iv) the Chief Financial Officer; or (v) such other personnel as may be prescribed. (2) Nothing contained in sub-section (1) shall prevent the data fiduciary from assigning any other function to the data protection officer, which it may consider necessary. (3) The data protection officer appointed under sub-section (1) shall be based in India and shall represent the data fiduciary under this Act.	
34.	***Clause 31: Processing by entities other than data fiduciaries***	***Clause 31: Processing by entities other than data fiduciaries***	• No change.

	(1) The data fiduciary shall not engage, appoint, use or involve a data processor to process personal data on its behalf without a contract entered into by the data fiduciary and such data processor. (2) The data processor referred to in sub-section (1) shall not engage, appoint, use, or involve another data processor in the processing on its behalf, except with the authorisation of the data fiduciary and unless permitted in the contract referred to in sub-section (1). *(3)* The data processor, and any employee of the data fiduciary or the data processor, shall only process personal data in accordance with the instructions of the data fiduciary and treat it confidential.	(1) The data fiduciary shall not engage, appoint, use or involve a data processor to process personal data on its behalf without a contract entered into by the data fiduciary and such data processor. (2) The data processor referred to in sub-section (1) shall not engage, appoint, use, or involve another data processor in the processing on its behalf, except with the authorisation of the data fiduciary and unless permitted in the contract referred to in sub-section (1). (3) The data processor, and any employee of the data fiduciary or the data processor, shall only process personal data in accordance with the instructions of the data fiduciary and treat it as confidential.	
35.	***Clause 32: Grievance redressal by data fiduciary*** (1) Every data fiduciary shall have in place the procedure and effective mechanisms to redress the grievances of data principals efficiently and in a speedy manner. (2) A data principal may make a complaint of contravention of any of the provisions of this Act or the rules or regulations made thereunder, which has caused or is likely to cause harm to such data principal, to— *(a)* the data protection officer, in case of a significant data fiduciary; or *(b)* an officer designated for this purpose, in case of any other data fiduciary.	***Clause 32: Grievance redressal by data fiduciary*** (1) Every data fiduciary shall have in place the procedure and effective mechanisms to redress the grievances of data principals efficiently and in a speedy manner. (2) A data principal may make a complaint of contravention of any of the provisions of this Act or the rules or regulations made thereunder, which has caused or is likely to cause harm to such data principal, to— *(a)* the data protection officer, in case of a significant data fiduciary; or *(b)* an officer designated for this purpose, in case of any other data fiduciary.	• The JPC observes that the manner in which complaints are to be filed before the DPA is not made out in the Bill. (para 2.141) • The JPC recommends a single window system to deal with complaints/ penalties/ compensation- in Clause 62, and makes consequential changes here. (para 2.142)

	(3) A complaint made under sub-section (2) shall be resolved by the data fiduciary in an expeditious manner and not later than thirty days from the date of receipt of the complaint by such data fiduciary. (4) Where a complaint is not resolved within the period specified under sub-section (3), or where the data principal is not satisfied with the manner in which the complaint is resolved, or the data fiduciary has rejected the complaint, the data principal may file a complaint to the Authority in such manner as may be prescribed.	(3) A complaint made under sub-section (2) shall be resolved by the data fiduciary in an expeditious manner and not later than thirty days from the date of receipt of the complaint by such data fiduciary. (4) Where a complaint is not resolved within the period specified under sub-section (3), or where the data principal is not satisfied with the manner in which the complaint is resolved, or the data fiduciary has rejected the complaint, the data principal may file a complaint to the Authority (***) under section 62.	
CHAPTER VII: RESTRICTION ON TRANSFER OF PERSONAL DATA OUTSIDE INDIA			
36.	***Clause 33: Prohibition on processing of sensitive personal data and critical personal data outside India*** (1) Subject to the conditions in sub-section (1) of section 34, the sensitive personal data may be transferred outside India, but such sensitive personal data shall continue to be stored in India. (2) The critical personal data shall only be processed in India. *Explanation.*—For the purposes of sub-section (2), the expression "critical personal data" means such personal data as may be notified by the Central Government to be the critical personal data	***Clause 33: Prohibition on processing of sensitive personal data and critical personal data outside India.*** (1) Subject to the conditions provided in sub-section (1) of section 34, the sensitive personal data may be transferred outside India, but such sensitive personal data shall continue to be stored in India. (2) The critical personal data shall only be processed in India. *Explanation.*—For the purposes of sub-section (2), the expression "critical personal data" means such personal data as may be notified by the Central Government to be the critical personal data.	• The JPC does not make any major edits to clause 33, it advocates for data localization to address the risks of cross-border data transfers and to fulfill India's strategic objectives in national security, privacy and building a domestic data economy. (para 1.9) The JPC sets out the objectives and key stakeholders involved in data localization. (para 1.9.4, 1.9.5) It recommends that India moves gradually towards data localization and calls upon the central government to work with sectoral regulators to develop a comprehensive data localization policy. (para 1.9.3, 1.9.6). • The JPC also recommends that concrete steps be taken by the government to ensure that a mirror copy of the sensitive personal data (**SPD**) and critical personal data (**CPD**) which is already in possession of the foreign

			entities be mandatorily brought to India in a time bound manner. (para 1.15.17.5)
37.	***Clause 34: Conditions for transfer of sensitive personal data and critical personal data.*** (1) The sensitive personal data may only be transferred outside India for the purpose of processing, when explicit consent is given by the data principal for such transfer, and where— *(a)* The transfer is made pursuant to a contract or intra-group scheme approved by the Authority: Provided that such contract or intra-group scheme shall not be approved, unless it makes the provisions for— (i) effective protection of the rights of the data principal under this Act, including in relation to further transfer to any other person; and (ii) liability of the data fiduciary for harm caused due to non-compliance of the provisions of such contract or intra-group scheme by such transfer; or *(b)* The Central Government, after consultation with the Authority, has allowed the transfer to a country or, such entity or class of entity in a country or, an international organisation on the basis of its finding that— (i) such sensitive personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements; and	***Clause 34: Conditions for transfer of sensitive personal data and critical personal data*** (1) The sensitive personal data may only be transferred outside India for the purpose of processing, when explicit consent is given by the data principal for such transfer, and where— *(a)* the transfer is made pursuant to a contract or intra-group scheme approved by the Authority in consultation with the Central Government: Provided that such contract or intra-group scheme shall not be approved, if the object of such transfer is against public policy or State policy and unless it makes the provisions for— (i) effective protection of the rights of the data principal under this Act, including in relation to further transfer to any other person; and (ii) liability of the data fiduciary for harm caused due to non-compliance of the provisions of such contract or intra-group scheme by such transfer; (***) *(b)* The Central Government, after consultation with the Authority, has allowed the transfer to a country or, such entity or class of (***) entities in a country or, an international organisation on the basis of its finding that–	• The JPC recommends amending Clause 34(1)(a) to include the phrase "in consultation with the Central Government" to ensure that transfer of any information outside the country is always in consultation with the Central Government. (para 2.149) • Additionally, transfers pursuant to contracts / intra-group schemes for cross border data transfer will not be approved if they are against the public policy of India (para 2.129, 2.150, 2.154) • An explanation for "public policy" is added in the provision. (para 2.151) • The JPC observes that the shifting nature of international relations merits the addition of a clause to ensure that foreign entities are restricted from sharing SPD with a third country or agency, unless such sharing is approved by the Central Government. It introduces this as one of the 3 conditions in the Central Government making a decision on adequacy. This appears to be aimed at restricting onward transfers to third countries. (para 2.154, 2.155)

	(ii) such transfer shall not prejudicially affect the enforcement of relevant laws by authorities with appropriate jurisdiction: Provided that any finding under this clause shall be reviewed periodically in such manner as may be prescribed; *(c)* the Authority has allowed transfer of any sensitive personal data or class of sensitive personal data necessary for any specific purpose. (2) Notwithstanding anything contained in sub-section (2) of section 33, any critical personal data may be transferred outside India, only where such transfer is— *(a)* to a person or entity engaged in the provision of health services or emergency services where such transfer is necessary for prompt action under section 12; or *(b)* to a country or, any entity or class of entity in a country or, to an international organisation, where the Central Government has deemed such transfer to be permissible under clause (b) of sub-section (1) and where such transfer in the opinion of the Central Government does not prejudicially affect the security and strategic interest of the State. (3) Any transfer under clause (a) of sub-section (2) shall be notified to the Authority within such period as may be specified by regulations.	(i) such sensitive personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements; (***) (ii) such transfer shall not prejudicially affect the enforcement of relevant laws by authorities with appropriate jurisdiction; and (iii) such sensitive personal data shall not be shared with any foreign government or agency unless such sharing is approved by the Central Government: Provided that any finding under this clause shall be reviewed periodically in such manner as may be prescribed; or *(c)* the Authority, in consultation with the Central Government, has allowed transfer of any sensitive personal data or class of sensitive personal data necessary for any specific purpose. *Explanation.*- For the purposes of this sub-section, an act is said to be against "public policy" or "State policy", if the said act promotes the breach of any law or is not in consonance with any public policy or State policy in this regard or has a tendency to harm the interest of the State or its citizens. (2) Notwithstanding anything contained in sub-section (2) of section 33, any critical personal data may be transferred outside India, only where such transfer is— *(a)* to a person or entity engaged in the provision of health services or emergency services where such	

		transfer is necessary for prompt action under section 12; or *(b)* to a country or, any entity or class of (***) entities in a country or, to an international organisation, where the Central Government has deemed such transfer to be permissible under clause (b) of sub-section (1) and where such transfer in the opinion of the Central Government does not prejudicially affect the security and strategic interests of the State. (3) Any transfer under clause (a) of sub-section (2) shall be (***) informed to the Authority within such period as may be specified by regulations.	
	CHAPTER VIII: EXEMPTIONS		
38.	***Clause 35: Power of the Central Government to exempt any agency of Government from application of the Act.*** Where the Central Government is satisfied that it is necessary or expedient,— (i) in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order; or (ii) for preventing incitement to the commission of any cognizable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, it may, by order, for reasons to be recorded in writing, direct that all or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data, as may be specified in the order subject to such procedure, safeguards and	***Clause 35: Power of the Central Government to exempt any agency of Government from application of the Act.*** Notwithstanding anything contained in any law for the time being in force, where the Central Government is satisfied that it is necessary or expedient,— (i) in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States **or** public order; or (ii) for preventing incitement to the commission of any cognizable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States **or** public order, it may, by order, for reasons to be recorded in writing, direct that all or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data, as may be specified in	• The JPC discusses the need to balance provisions of the bills with concerns of national security. It references the Puttaswamy judgment which sets out a test to determine if state intervention infringes the right to privacy. (para 2.158, 2.159, 2.160) • The JPC also studies similar provisions in global data protection legislations (Singapore, China, US, EU), noting that state intervention is allowed under certain specific circumstances. The Report notes that MEITY submitted to the JPC that provisions permitting state intervention are in line with the reasonable restrictions set out in Article 19(2) of the Constitution. (para 2.162-2.165; 2.170)

	oversight mechanism to be followed by the agency, as may be prescribed. *Explanation*. —For the purposes of this section, — (i) the term "cognizable offence" means the offence as defined in clause (c) of section 2 of the Code of Criminal Procedure, 1973; (ii) the expression "processing of such personal data" includes sharing by or sharing with such agency of the Government by any data fiduciary, data processor or data principal;	the order subject to such procedure, safeguards and oversight mechanism to be followed by the agency, as may be prescribed. *Explanation*. —For the purposes of this section, — (i) the term "cognizable offence" means the offence as defined in clause (c) of section 2 of the Code of Criminal Procedure, 1973; (ii) the expression "processing of such personal data" includes sharing by or sharing with such agency of the Government by any data fiduciary, data processor or data principal; and (iii) the expression "such procedure" refers to just, fair, reasonable and proportionate procedure.	• The JPC recommends amendments to Clause 35 to reflect the need to strike a balance by adding qualifying terms "just, fair, reasonable and proportionate"to the procedure that needs to be followed by the government. (para 2.171)
39.	***Clause 36:Exemption of certain provisions for certain processing of personal data*** The provisions of Chapter II except Section 4, Chapters III to V, Chapter VI except section 24, and Chapter VII shall not apply where— *(a)* personal data is processed in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of any law for the time being in force; *(b)* disclosure of personal data is necessary for enforcing any legal right or claim, seeking any relief, defending any charge, opposing any claim, or obtaining any legal advice from an advocate in any impending legal proceeding; *(c)* processing of personal data by any court or tribunal in India is necessary for the exercise of any judicial function;	***Clause 36: Exemption of certain provisions for certain processing of personal data*** The provisions of Chapter II (***) to VII, except section 24, shall not apply where— *(a)* The personal data is processed in the interests of prevention, detection, investigation and prosecution of any offence or (***) contravention of any law for the time being in force; *(b)* the disclosure of personal data is necessary for enforcing any legal right or claim, seeking any relief, defending any charge, opposing any claim, or obtaining any legal advice from an advocate in any impending legal proceeding; *(c)* the processing of personal data by any court or tribunal in India is necessary for the exercise of any judicial function; *(d)* the personal data is processed by a natural person for any personal or domestic purpose, except	• The JPC recommends changes to simplify language used in the Bill. (para 2.176) • The JPC also examines the processing of personal data for journalistic purpose and notes that while free speech is vital to media, the Bill also must protect against misuse of these provisions. It further observes that self-regulation is insufficient and entities like the Press Council of India are ill-equipped to handle journalism through new media such as social media and the internet. The JPC accordingly calls for a comprehensive code and the establishment of a statutory regulatory body. (para 2.177)

	(d) personal data is processed by a natural person for any personal or domestic purpose, except where such processing involves disclosure to the public, or is undertaken in connection with any professional or commercial activity; or *(e)* processing of personal data is necessary for or relevant to a journalistic purpose, by any person and is in compliance with any code of ethics issued by the Press Council of India, or by any media self-regulatory organisation.	where such processing involves disclosure to the public, or is undertaken in connection with any professional or commercial activity; or *(e)* the processing of personal data is necessary for or relevant to a journalistic purpose, by any person and is in compliance with the rules and regulations made under this Act, (***) code of ethics issued by the Press Council of India, or by any statutory media (***) regulatory organisation.	
40.	***Clause 37:Power of the Central Government to exempt certain data processors*** The Central Government may, by notification, exempt from the application of this Act, the processing of personal data of data principals not within the territory of India, pursuant to any contract entered into with any person outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law.	***Clause 37: Power of the Central Government to exempt certain data processors*** The Central Government may, by notification, exempt from the application of this Act, the processing of personal data of data principals not within the territory of India, pursuant to any contract entered into with any person outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law.	• No change.
41.	***Clause 38: Exemption for research, archiving or statistical purposes.*** Where the processing of personal data is necessary for research, archiving, or statistical purposes, and the Authority is satisfied that— *(a)* the compliance with the provisions of this Act shall disproportionately divert resources from such purpose; *(b)* the purposes of processing cannot be achieved if the personal data is anonymised;	***Clause 38: Exemption for research, archiving or statistical purposes.*** Where the processing of personal data is necessary for research, archiving, or statistical purposes, and the Authority is satisfied that— *(a)* the compliance with the provisions of this Act shall disproportionately divert resources from such purpose; *(b)* the purposes of processing cannot be achieved if the personal data is anonymised;	• No change.

	(c) the data fiduciary has carried out de-identification in accordance with the code of practice specified under section 50 and the purpose of processing can be achieved if the personal data is in de-identified form; *(d)* the personal data shall not be used to take any decision specific to or action directed to the data principal; and *(e)* the personal data shall not be processed in the manner that gives rise to a risk of significant harm to the data principal, it may, by notification, exempt such class of research, archiving, or statistical purposes from the application of any of the provisions of this Act as may be specified by regulations	*(c)* the data fiduciary has carried out de-identification in accordance with the code of practice specified under section 50 and the purpose of processing can be achieved if the personal data is in de-identified form; *(d)* the personal data shall not be used to take any decision specific to or action directed to the data principal; and *(e)* the personal data shall not be processed in the manner that gives rise to a risk of significant harm to the data principal, it may, by notification, exempt such class of research, archiving, or statistical purposes from the application of any of the provisions of this Act as may be specified by regulations.	
42.	***Clause 39:Exemption for manual processing by small entities.*** (1) The provisions of sections 7, 8, 9, clause (c) of sub-section (1) of section 17 and sections 19 to 32 shall not apply where the processing of personal data by a small entity is not automated. (2) For the purposes of sub-section (1), a "small entity" means such data fiduciary as may be classified, by regulations, by Authority, having regard to— *(a)* the turnover of data fiduciary in the preceding financial year; *(b)* the purpose of collection of personal data for disclosure to any other individuals or entities; and ***(a)*** the volume of personal data processed by such data fiduciary in any one day in the preceding twelve calendar months.	***Clause 39: Exemption for (***) non-automated processing by small entities.*** (1) The provisions of sections 7, 8, 9, clause (c) of sub-section (1) of section 17 and sections 19 to 32 shall not apply where the processing of personal data by a small entity is not automated. (2) For the purposes of sub-section (1), a "small entity" means such data fiduciary as may be classified, by regulations, by Authority, having regard to— *(b)* the turnover of data fiduciary in the preceding financial year; *(c)* the purpose of collection of personal data for disclosure to any other individuals or entities; and *(d)* the volume of personal data processed by such data fiduciary in any one day in the preceding twelve calendar months.	• The JPC notes that term "manual processing" used in the margin heading of Clause 39 has not been used anywhere and recommends changing it to "non-automated" to remove ambiguity. (para 2.181)

43.	***Clause 40: Sandbox for encouraging innovation etc.*** (1) The Authority shall, for the purposes of encouraging innovation in artificial intelligence, machine-learning or any other emerging technology in public interest, create a Sandbox. (2) Any data fiduciary whose privacy by design policy is certified by the Authority under sub-section (3) of section 22 shall be eligible to apply, in such manner as may be specified by regulations, for inclusion in the Sandbox created under sub-section (1). (3) Any data fiduciary applying for inclusion in the Sandbox under sub-section (2) shall furnish the following information, namely:— *(a)* the term for which it seeks to utilise the benefits of Sandbox, provided that such term shall not exceed twelve months; *(b)* the innovative use of technology and its beneficial uses; *(c)* the data principals or categories of data principals participating under the proposed processing; and *(d)* any other information as may be specified by regulations. (4) The Authority shall, while including any data fiduciary in the Sandbox, specify— *(a)* the term of the inclusion in the Sandbox, which may be renewed not more than twice, subject to a total period of thirty-six months; *(b)* the safeguards including terms and conditions in view of the obligations under clause (c) including the requirement of consent of data principals	***Clause 40: Sandbox for encouraging innovation etc.*** (1) The Authority (***) may, for the purposes of encouraging innovation in artificial intelligence, machine-learning or any other emerging technology in public interest, create a Sandbox. (2) Any data fiduciary as well as start-ups whose privacy by design policy is certified by the Authority under sub-section (3) of section 22 shall be eligible to apply, in such manner as may be specified by regulations, for inclusion in the Sandbox created under sub-section (1). (3) Any data fiduciary applying for inclusion in the Sandbox under sub-section (2) shall furnish the following information, namely:— *(a)* the term for which it seeks to utilise the benefits of Sandbox, provided that such term shall not exceed twelve months; *(b)* the innovative use of technology and its beneficial uses; *(c)* the data principals or categories of data principals participating under the proposed processing; and *(d)* any other information as may be specified by regulations. (4) The Authority shall, while including any data fiduciary in the Sandbox, specify— *(a)* the term of the inclusion in the Sandbox, which may be renewed not more than twice, subject to a total period of thirty-six months; *(b)* the safeguards including terms and conditions in view of the obligations under clause (c) including	• The JPC acknowledges the impact of certain aspects of the law on corporate innovation. It calls upon the DPA to be mindful of the interest of start-ups and encourage innovation and a regulatory sandbox when it frames regulations. (para 1.15.15.2) • The JPC also recommends that to encourage more innovations, simultaneously, the Patent Act, 1970 may also be amended. (para 1.15.15.2) • The JPC notes that the use of the word "shall" could impose a mandatory obligation upon the government to create a regulatory sandbox. It recommends changing this to "may", keeping in mind the fact that the government may not have the necessary infrastructure or expertise to establish a sandbox. (para 2.184) • The JPC explicitly includes start-ups in Clause 40(2) to allow them to actively participate in the sandbox regime and allow India to emerge as a $5 trillion economy. A definition of sandbox is added as an explanation to avoid misinterpretation or ambiguity. (para 2.185, 2.187)

	participating under any licensed activity, compensation to such data principals and penalties in relation to such safeguards; and *(c)* that the following obligations shall not apply or apply with modified form to such data fiduciary, namely:— (i) the obligation to specify clear and specific purposes under sections 4 and 5; (ii) limitation on collection of personal data under section 6; and (iii) any other obligation to the extent, it is directly depending on the obligations under sections 5 and 6; and (iv) the restriction on retention of personal data under section 9.	the requirement of consent of data principals participating under any licensed activity, compensation to such data principals and penalties in relation to such safeguards; and *(c)* that the following obligations shall not apply or apply with modified form to such data fiduciary, namely:— (i) the obligation to (***) comply with the provisions under sections 4 and 5; (ii) limitation on collection of personal data under section 6; and (iii) any other obligation to the extent, it is directly depending on (***) sections 5 and 6; and (iv) the restriction on retention of personal data under section 9. *Explanation*.- For the purposes of this Act, the expression "Sandbox" means such live testing of new products or services in a controlled or test regulatory environment for which the Authority may or may not permit certain regulatory relaxations for a specified period of time for the limited purpose of the testing.	
CHAPTER IX: DATA PROTECTION AUTHORITY OF INDIA			
44.	***Clause 41: Establishment of Authority*** (1) The Central Government shall, by notification, establish, for the purposes of this Act, an Authority to be called the Data Protection Authority of India. (2) The Authority referred to in sub-section (1) 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	***Clause 41: Establishment of Authority*** (1) The Central Government shall, by notification, establish, for the purposes of this Act, an Authority to be called the Data Protection Authority of India. (2) The Authority referred to in sub-section (1) 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	• No change.

	and dispose of property, both movable and immovable, and to contract and shall, by the said name, sue or be sued. (3) The head office of the Authority shall be at such place as may be prescribed. (4) The Authority may, with the prior approval of the Central Government, establish its offices at other places in India.	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 head office of the Authority shall be at such place as may be prescribed. (4) The Authority may, with the prior approval of the Central Government, establish its offices at other places in India.	
45.	***Clause 42: Composition and qualifications for appointment of Members.*** (1) The Authority shall consist of a Chairperson and not more than six whole-time Members, of which one shall be having qualifications and experience in law (2) The Chairperson and the Members of the Authority shall be appointed by the Central Government on the recommendation made by a selection committee consisting of— *(a)* the Cabinet Secretary, who shall be Chairperson of the selection committee; *(b)* the Secretary to the Government of India in the Ministry or Department dealing with the Legal Affairs; and *(c)* the Secretary to the Government of India in the Ministry or Department dealing with the Electronics and Information Technology; (3) The procedure to be followed by the Selection Committee for recommending the names under sub-section (2) shall be such as may be prescribed.	***Clause 42: Composition and qualifications for appointment of Chairperson and Members*** (1) The Authority shall consist of a Chairperson and not more than six whole-time Members, of which one shall be (***) an expert in the area of law having such qualifications and experience (***) as may be prescribed. (2) The Chairperson and the Members of the Authority shall be appointed by the Central Government on the recommendation made by a Selection Committee consisting of— (i) the Cabinet Secretary, who shall be Chairperson of the Selection Committee; (ii) the Attorney General of India - Member; (iii) the Secretary to the Government of India in the Ministry or Department dealing with the Legal Affairs - Member; (***) (iv) the Secretary to the Government of India in the Ministry or Department dealing with (***) Electronics and Information Technology - Member;	• The JPC recommends modifying Clause 42(1) to specify that a member of the DPA shall be a legal expert with such qualifications as may be prescribed. It also specifies the composition of the selection committee which will recommend members to the DPA. (para 2.189, 2.190) • The JPC observes that the proposed composition of the selection committee in the Bill are secretary level bureaucrats. The JPC recommends the inclusion of technical, legal, and academic experts to make the DPA inclusive, robust and inclusive. (para 2.191)

	(4) The Chairperson and the Members of the Authority shall be persons of ability, integrity and standing, and shall have qualification and specialised knowledge and experience of, and not less than ten years in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, public administration, national security or related subjects. *(5)* A vacancy caused to the office of the Chairperson or any other member of the Authority shall be filled up within a period of three months from the date on which such vacancy occurs.	(v) an independent expert to be nominated by the Central Government from the fields of data protection, information technology, data management, data science, data security, cyber and internet laws, public administration or related subjects - Member; (vi) a Director of any of the Indian Institutes of Technology to be nominated by the Central Government – Member; and (vii) a Director of any of the Indian Institutes of Management to be nominated by the Central Government – Member. (3) The procedure to be followed by the Selection Committee for recommending the names under sub-section (2) shall be such as may be prescribed. (4) The Chairperson and the Members of the Authority shall be persons of ability, integrity and standing, and shall have qualifications and specialised knowledge and experience of (***) not less than ten years in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, public administration, national security or related subjects. (5) A vacancy caused to the office of the Chairperson or any other Member of the Authority shall be filled up within a period of three months from the date on which such vacancy occurs.	
46.	***Clause 43: Terms and conditions of appointment***	***Clause 43: Terms and conditions of appointment***	• No change.

	(1) The Chairperson and the Members of the Authority shall be appointed for a term of five years or till they attain the age of sixty-five years, whichever is earlier, and they shall not be eligible for re-appointment. (2) The salaries and allowances payable to, and other terms and conditions of service of the Chairperson and the Members of the Authority shall be such as may be prescribed. (3) The Chairperson and the Members shall not, during their term and for a period of two years from the date on which they cease to hold office, accept— *(a)* any employment either under the Central Government or under any State Government; or *(b)* any appointment, in any capacity whatsoever, with a significant data fiduciary. (4) Notwithstanding anything contained in sub-section (1), the Chairperson or a Member of the Authority may— *(a)* relinquish his office by giving in writing to the Central Government a notice of not less than three months; or *(b)* be removed from his office in accordance with the provisions of this Act.	(1) The Chairperson and the Members of the Authority shall be appointed for a term of five years or till they attain the age of sixty-five years, whichever is earlier, and they shall not be eligible for re-appointment. (2) The salaries and allowances payable to, and other terms and conditions of service of the Chairperson and the Members of the Authority shall be such as may be prescribed. (3) The Chairperson and the Members shall not, during their term and for a period of two years from the date on which they cease to hold office, accept— *(a)* any employment either under the Central Government or under any State Government; or *(b)* any appointment, in any capacity whatsoever, with a significant data fiduciary. (4) Notwithstanding anything contained in sub-section (1), the Chairperson or a Member of the Authority may— *(a)* relinquish his office by giving in writing to the Central Government a notice of not less than three months; or *(b)* be removed from his office in accordance with the provisions of this Act.	
47.	***Clause 44: Removal of Chairperson or other Members.*** (1) The Central Government may remove from office, the Chairperson or any Member of the Authority who— *(a)* has been adjudged as an insolvent; *(b)* has become physically or mentally incapable of acting as a Chairperson or member;	***Clause 44: Removal of Chairperson or other Members.*** (1) The Central Government may remove from office, the Chairperson or any Member of the Authority who— *(a)* has been adjudged as an insolvent;	• The JPC recommends cosmetic changes and modifies "a reasonable opportunity of being heard" in Clause 44(2) to "an opportunity of being heard".

	(c) has been convicted of an offence, which in the opinion of the Central Government, involves moral turpitude; *(d)* has so abused their position as to render their continuation in office detrimental to the public interest; or *(e)* has acquired such financial or other interest as is likely to affect prejudicially their functions as a Chairperson or a Member. *(2)* No Chairperson or any Member of the Authority shall be removed under clause (d) or (e) of sub-section (1) unless he has been given a reasonable opportunity of being heard.	*(b)* has become physically or mentally incapable of acting as a Chairperson or Member; *(c)* has been convicted of an offence, which in the opinion of the Central Government, involves moral turpitude; *(d)* has so abused their position as to render their continuation in office detrimental to the public interest; or *(e)* has acquired such financial or other interest as is likely to affect prejudicially(***) his functions as a Chairperson or a Member. *(2)* No Chairperson or any Member of the Authority shall be removed under clause (d) or (e) of sub-section (1) unless he has been given an(***) opportunity of being heard.	
48.	***Clause 45: Powers of chairperson*** The Chairperson of the Authority shall have powers of general superintendence and direction of the affairs of the Authority and shall also exercise all powers and do all such acts and things which may be exercised or done by the Authority under this Act.	***Clause 45: Powers of chairperson*** The Chairperson of the Authority shall (***) have powers of general superintendence and direction in the conduct of the affairs of the Authority and he shall, **(***)** in addition to presiding over the meetings of the Authority, exercise all powers and do all such acts and things which may be exercised or done by the Authority under this Act.	• The JPC observes that Clause 45 does not specify the power of the Chairperson to preside over meetings of the DPA. Phrases have been added to categorically state the Chairperson's powers. (para 2.193)
49.	***Clause 46: Meetings of authority*** (1) The Chairperson and Members of the Authority shall meet at such times and places and shall observe such rules and procedures in regard to transaction of business at its meetings including quorum at such meetings, as may be prescribed.	***Clause 46: Meetings of authority*** (1) The Chairperson and Members of the Authority shall meet at such times and places and shall observe such rules and procedures in regard to transaction of business at its meetings including quorum at such meetings, as may be prescribed.	• The JPC recommends a cosmetic change to correct grammar.

	(2) If, for any reason, the Chairperson is unable to attend any meeting of the Authority, any other Member chosen by the Members present at the meeting, shall preside the meeting. (3) All questions which come up before any meeting of the Authority shall be decided by a majority of votes of the Members present and voting, and in the event of an equality of votes, the Chairperson or in his absence, the member presiding, shall have the right to exercise a second or casting vote. (4) Any Member who has any direct or indirect pecuniary interest in any matter coming up for consideration at a meeting of the Authority shall disclose the nature of his interest at such meeting, which shall be recorded in the proceedings of the Authority and such Member shall not take part in any deliberation or decision of the Authority with respect to that matter.	(2) If, for any reason, the Chairperson is unable to attend any meeting of the Authority, any other Member chosen by the Members present at the meeting, shall preside **over** the meeting. (3) All questions which come up before any meeting of the Authority shall be decided by a majority of votes of the Members present and voting, and in the event of an equality of votes, the Chairperson or in his absence, the Member presiding, shall have the right to exercise a second or casting vote. (4) Any Member who has any direct or indirect pecuniary interest in any matter coming up for consideration at a meeting of the Authority shall disclose the nature of his interest at such meeting, which shall be recorded in the proceedings of the Authority and such Member shall not take part in any deliberation or decision of the Authority with respect to that matter.	
50.	***Clause 47: Vacancies, etc., not to invalidate proceedings of Authority*** No act or proceeding of the Authority shall be invalid merely by reason of— *(a)* any vacancy or defect in the constitution of the Authority; *(b)* any defect in the appointment of a person as a Chairperson or Member; or *(c)* any irregularity in the procedure of the Authority not affecting the merits of the case	***Clause 47: Vacancies, etc., not to invalidate proceedings of Authority*** No act or proceeding of the Authority shall be invalid merely by reason of— *(a)* any vacancy or defect in the constitution of the Authority; *(b)* any defect in the appointment of a person as a Chairperson or Member; or *(c)* any irregularity in the procedure of the Authority not affecting the merits of the case	• No change.
51.	***Clause 48: Officers and other employees of Authority***	***Clause 48: Officers and other employees of Authority***	• The JPC recommends a cosmetic change to correct grammar.

	(1) The Authority may appoint such officers, other employees, consultants and experts as it may consider necessary for effectively discharging of its functions under this Act. (2) Any remuneration, salary or allowances, and other terms and conditions of service of such officers, employees, consultants and experts shall be such as may be specified by regulations.	(1) The Authority may appoint such officers, other employees, consultants and experts as it may consider necessary for effectively discharging (***) its functions under this Act. (2) Any remuneration, salary or allowances, and other terms and conditions of service of such officers, employees, consultants and experts shall be such as may be specified by regulations.	
52.	***Clause 49: Powers and functions of Data Protection Authority*** (1) It shall be the duty of the Authority to protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of this Act, and promote awareness about data protection. (2) Without prejudice to the generality of the foregoing and other functions under this Act, the functions of the Authority shall include— *(a)* monitoring and enforcing application of the provisions of this Act; *(b)* taking prompt and appropriate action in response to personal data breach in accordance with the provisions of this Act; *(c)* maintaining a database on its website containing names of significant data fiduciaries along with a rating in the form of a data trust score indicating compliance with the obligations of this Act by such fiduciaries; *(d)* examination of any data audit reports and taking any action pursuant thereto;	***Clause 49: Powers and functions of Data Protection Authority*** (1) It shall be the duty of the Authority to protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of this Act, and promote awareness about data protection. (2) Without prejudice to the generality of the foregoing and other functions under this Act, the functions of the Authority shall include— *(a)* monitoring and enforcing application of the provisions of this Act and the rules and regulations made thereunder; *(b)* taking prompt and appropriate action in response to (***) data breach in accordance with the provisions of this Act; *(c)* maintaining a database on its website containing names of significant data fiduciaries along with a rating in the form of a data trust score indicating compliance with the obligations of this Act by such fiduciaries;	• The JPC expresses its concerns over hardware integrity and how attacks through hardware are potentially more harmful due to their rarity and the lack of regulation for it. In this context, the report notes MEITY's submission that India has a device evaluation framework that all device manufacturers must go through before a device can be sold in India. (para 2.196, 2.197, 2.198) • The JPC, however, notes that the lack of awareness about hardware integrity could open Indian users to privacy violations. It considers the global decentralized nature of manufacturing and the advent of Internet of Things (IoT) and smart devices in daily life, and recommends that the DPA devise a framework and authorize an appropriate agency to monitor, test and certify the integrity of hardware equipment. This is inserted at Clause 49(2)(o). (paras 1.15.16.3 and 2.201) • The JPC recommends that the word "personal" be deleted from Clause 49 (2) (b)

	(e) issuance of a certificate of registration to data auditors and renewal, withdrawal, suspension or cancellation thereof and maintaining a database of registered data auditors and specifying the qualifications, code of conduct, practical training and functions to be performed by such data auditors; *(f)* classification of data fiduciaries; *(g)* monitoring cross-border transfer of personal data; *(h)* specifying codes of practice; *(i)* promoting awareness and understanding of the risks, rules, safeguards and rights in respect of protection of personal data amongst data fiduciaries and data principals; *(j)* monitoring technological developments and commercial practices that may affect protection of personal data; *(k)* promoting measures and undertaking research for innovation in the field of protection of personal data; *(l)* advising Central Government, State Government and any other authority on measures required to be taken to promote protection of personal data and ensuring consistency of application and enforcement of this Act; *(m)* specifying fees and other charges for carrying out the purposes of this Act; *(n)* receiving and inquiring complaints under this Act; *(o)* performing such other functions as may be prescribed. *(3)* Where, pursuant to the provisions of this Act, the Authority processes any personal data, it shall be construed as the data fiduciary or the data processor in relation to such personal data as applicable, and	*(d)* examination of any data audit reports and taking any action pursuant thereto; *(e)* issuance of a certificate of registration to data auditors and renewal, withdrawal, suspension or cancellation thereof and maintaining a database of registered data auditors and specifying the qualifications, code of conduct, practical training and functions to be performed by such data auditors; *(f)* classification of data fiduciaries; *(g)* monitoring cross-border transfer of personal data; *(h)* specifying codes of practice; *(i)* promoting awareness and understanding of the risks, rules, safeguards and rights in respect of protection of personal data amongst data fiduciaries and data principals; *(j)* monitoring technological developments and commercial practices that may affect protection of personal data; *(k)* promoting measures and undertaking research for innovation in the field of protection of personal data; *(l)* advising Central Government, State Government and any other authority on measures required to be taken to promote protection of personal data and ensuring consistency of application and enforcement of this Act; *(m)* specifying fees and other charges for carrying out the purposes of this Act; *(n)* receiving and inquiring complaints under this Act; **(***)** *(o)* monitoring, testing and certification by an appropriate agency authorized by the Central Government for this purpose to ensure integrity and trustworthiness of hardware and software on	to reflect the expanded scope of the Bill to encompass personal and non-personal data. (para 2.200)

	where the Authority comes into possession of any information that is treated as confidential by the data fiduciary or data processor, it shall not disclose such information unless required	computing devices to prevent any malicious insertion that may cause data breach; and *(p)* performing such other functions as may be prescribed. *(3)* Where, pursuant to the provisions of this Act, the Authority processes any personal data, it shall be construed as the data fiduciary or the data processor in relation to such personal data as applicable, and where the Authority comes into possession of any information that is treated as confidential by (***) such data fiduciary or data processor, it shall not disclose such information unless required.	
53.	***Clause 50: Codes of Practice*** (1) The Authority shall, by regulations, specify codes of practice to promote good practices of data protection and facilitate compliance with the obligations under this Act. (2) Notwithstanding anything contained in sub-section (1), the Authority may approve any code of practice submitted by an industry or trade association, an association representing the interest of data principals, any sectoral regulator or statutory Authority; or any **d**epartments or **m**inistries of the Central or State Government. (3) The Authority shall ensure transparency and compliance with the obligations of data fiduciary and the rights of the data principal under this Act while specifying or approving any code of practice under this section.	***Clause 50: Codes of Practice*** (1) The Authority shall, by regulations, specify codes of practice to promote good practices of data protection and facilitate compliance with the obligations under this Act. (2) Notwithstanding anything contained in sub-section (1), the Authority may approve any code of practice submitted by- (i) the associations representing- (a) technical services organizations; (b) (***) industry or trade (***) (c) (***) the interest of data principals (ii) any sectoral regulator or statutory Authority; or	• The JPC acknowledges suggestions from stakeholders to empower self-regulatory associations to develop standards for governance and technical specifications as may be necessary. So, it recommends that associations representing technical services organisations could also submit codes of practice that are approved and adopted by the DPA (para 2.204, 2.205, 2.206). • The JPC recommends expanding the power of the DPA to cover action to be taken by DFs and processors in case of all data breaches, not just personal data breaches- in line with its recommendations on data breaches. (para 2.207)

	(4) A code of practice under sub-section (1) or sub-section (2), shall not be issued unless the Authority has made consultation with the sectoral regulators and other stakeholders including the public and has followed such procedure as may be prescribed. (5) A code of practice issued under this section shall not derogate from the provisions of this Actor any other law for the time being in force. (6) The code of practice under this Act may include the following matters, namely:— *(a)* requirements for notice under section 7 including any model forms or guidance relating to notice; *(b)* measures for ensuring quality of personal data processed under section 8; *(c)* measures pertaining to the retention of personal data under section 9; *(d)* manner for obtaining valid consent under section 11; *(e)* processing of personal data under section 12; *(f)* activities where processing of personal data may be undertaken under section 14; *(g)* processing of sensitive personal data under Chapter III; *(h)* processing of personal data under any other ground for processing, including processing of personal data of children and age-verification under this Act; *(i)* exercise of any right by data principals under Chapter V; *(j)* the standards and means by which a data principal may avail the right to data portability under section 19; *(k)* transparency and accountability measures including the standards thereof to be maintained by	(iii) any Departments or Ministries of the Central Government or State Government. (3) The Authority shall ensure transparency and compliance with the obligations of data fiduciary and the rights of the data principal under this Act while specifying or approving any code of practice under this section. (4) A code of practice under sub-section (1) or sub-section (2), shall not be issued unless the Authority has made consultation with the sectoral regulators and other stakeholders including the public and has followed such procedure as may be prescribed. (5) A code of practice issued under this section shall not derogate from the provisions of this Actor any other law for the time being in force. (6) The code of practice under this Act may include the following matters, namely:— *(a)* requirements for notice under section 7 including any model forms or guidance relating to notice; *(b)* measures for ensuring quality of personal data processed under section 8; *(c)* measures pertaining to the retention of personal data under section 9; *(d)* manner for obtaining valid consent under section 11; *(e)* processing of personal data under section 12; *(f)* activities where processing of personal data may be undertaken under section 14; *(g)* processing of sensitive personal data under Chapter III;	

	data fiduciaries and data processors under Chapter VI; *(l)* standards for security safeguards to be maintained by data fiduciaries and data processors under section 24; *(m)* methods of de-identification and anonymisation; *(n)* methods of destruction, deletion, or erasure of personal data where required under this Act; *(o)* appropriate action to be taken by the data fiduciary or data processor in response to a personal data breach under section 25; *(p)* manner in which data protection impact assessments may be carried out by the data fiduciary or a class thereof under section 27; *(q)* transfer of personal data outside India pursuant to section 34; *(r)* processing of any personal data or sensitive personal data to carry out any activity necessary for research, archiving or statistical purposes under section 38; and *(s)* any other matter which, in the view of the Authority, may be necessary or relevant to be provided in the code of practice. *(7)* The Authority may review, modify or revoke a code of practice issued under this section in such manner as may be prescribed.	*(h)* processing of personal data under any other ground for processing, including processing of personal data of children and age-verification under this Act; *(i)* exercise of any right by data principals under Chapter V; *(j)* the standards and means by which a data principal may avail the right to data portability under section 19; *(k)* transparency and accountability measures including the standards thereof to be maintained by data fiduciaries and data processors under Chapter VI; *(l)* standards for security safeguards to be maintained by data fiduciaries and data processors under section 24; *(m)* methods of de-identification and anonymisation; *(n)* methods of destruction, deletion, or erasure of personal data where required under this Act; *(o)* appropriate action to be taken by the data fiduciary or data processor in response to a (***) data breach under section 25; *(p)* manner in which data protection impact assessments may be carried out by the data fiduciary or a class thereof under section 27; *(q)* transfer of personal data outside India pursuant to section 34; *(r)* processing of any personal data or sensitive personal data to carry out any activity necessary for research, archiving or statistical purposes under section 38; and *(s)* any other matter which, in (***) view of the Authority, may be necessary or relevant to be provided in the code of practice.	

		(7) The Authority may review, modify or revoke a code of practice issued under this section in such manner as may be prescribed.	
54.	***Clause 51: Power of Authority to issue directions*** (1) The Authority may, for the discharge of its functions under this Act, issue such directions from time to time as it may consider necessary to any data fiduciary or data processor who shall be bound to comply with such directions. (2) No direction shall be issued under sub-section (1) unless the Authority has given has given a reasonable opportunity of being heard to the data fiduciaries or data processor. (3) The Authority may, on a representation made to it or on its own motion, modify, suspend, withdraw or cancel any direction issued under sub-section (1) and in doing so, may impose such conditions as it deems fit, subject to which the modification, suspension, withdrawal or cancellation shall have effect.	***Clause 51: Power of Authority to issue directions*** (1) The Authority may, for the discharge of its functions under this Act, issue such directions from time to time as it may consider necessary to any data fiduciary or data processor who shall be bound to comply with such directions. (2) No direction shall be issued under sub-section (1) unless the Authority has given an (***) opportunity of being heard to the data fiduciary (***) or the data processor concerned. *(3)* The Authority may, on a representation made to it or on its own motion, modify, suspend, withdraw or cancel any direction issued under sub-section (1) and in doing so, may impose such conditions as it deems fit, subject to which the modification, suspension, withdrawal or cancellation shall have effect.	• The JPC modifies "a reasonable opportunity of being heard" in Clause 51(2) to "an opportunity of being heard".
55.	***Clause 52: Power of Authority to call for information.*** (1) Without prejudice to the other provisions of this Act, the Authority may require a data fiduciary or data processor to provide such information as may be reasonably required by it for discharging its functions under this Act. (2) If the Authority requires a data fiduciary or a data processor to provide any information under sub-	***Clause 52: Power of Authority to call for information*** (1) Without prejudice to the other provisions of this Act, the Authority may require a data fiduciary or data processor to provide such information as may be reasonably required by it for discharging its functions under this Act. (2) If the Authority requires a data fiduciary or a data processor to provide any information under sub-	• No change.

	section (1), it shall provide a notice in writing to the data fiduciary or the data processor stating the reasons for such requisition. (3) The Authority shall, by regulations, specify the manner in which the data fiduciary or data processor shall provide the information sought in sub-section (1), including the designation of the officer or employee of the Authority who may seek such information, the period within which such information is to be furnished and the form in which such information may be provided.	section (1), it shall provide a notice in writing to the data fiduciary or the data processor stating the reasons for such requisition. (3) The Authority shall, by regulations, specify the manner in which the data fiduciary or data processor shall provide the information sought in sub-section (1), including the designation of the officer or employee of the Authority who may seek such information, the period within which such information is to be furnished and the form in which such information may be provided.	
56.	***Clause 53: Power of Authority to conduct inquiry*** (1) The Authority may, on its own or on a complaint received by it, inquire or cause to be inquired, if it has reasonable grounds to believe that— *(a)* the activities of the data fiduciary or data processor are being conducted in a manner which is detrimental to the interest of data principals; or *(b)* any data fiduciary or data processor has contravened any of the provisions of this Act or the rules or regulations made thereunder, or any direction of the Authority. (2) For the purposes of sub-section (1), the Authority shall, by an order in writing, appoint one of its officers as an Inquiry Officer to inquire into the affairs of such data fiduciary or data processor and to report to the Authority on any inquiry made. (3) For the purpose of any inquiry under this section, the Inquiry Officer may, wherever necessary, seek the assistance of any other person.	***Clause 53: Power of Authority to conduct inquiry*** (1) The Authority may, on its own or on a complaint received by it, inquire or cause to be inquired, if it has reasonable grounds to believe that— *(a)* the activities of the data fiduciary or data processor are being conducted in a manner which is detrimental to the interests of data principals; or *(b)* any data fiduciary or data processor has contravened any of the provisions of this Act or the rules or regulations made thereunder, or any direction of the Authority. (2) For the purposes of sub-section (1), the Authority shall, by an order in writing, appoint one of its officers as an Inquiry Officer to inquire into the affairs of such data fiduciary or data processor and to report to the Authority on any inquiry made. (3) For the purpose of any inquiry under this section, the Inquiry Officer may, wherever necessary, seek the assistance of any other person.	• The JPC only makes cosmetic changes to the clause.

	(4) The order referred to in sub-section (2) shall specify the reasons for the inquiry and the scope of the inquiry and may be modified from time to time. (5) Every officer, employee or other person acting under the direct authority of the data fiduciary or the data processor, or a service provider, or a contractor, where services are being obtained by or provided to the data fiduciary or data processor, as the case may be, shall be bound to produce before the Inquiry Officer, all such books, registers, documents, records and any data in their custody or power and to furnish to the Inquiry Officer any statement and information relating to the affairs of the data fiduciary or data processor as the Inquiry Officer may require within such time as the said Inquiry Officer may specify. (6) The Inquiry Officer shall provide a notice in writing to the persons referred to in sub-section (5) stating the reasons thereof and the relationship between the data fiduciary and the Inquiry Officer. (7) The Inquiry Officer may keep in its custody any books, registers, documents, records and other data produced under sub-section (5) for six months and thereafter shall return the same to the person by whom or on whose behalf such books, registers, documents, records and data are produced, unless an approval to retain such books, registers, documents, record and data for an additional period not exceeding three months has been obtained from the Authority. (8) Notwithstanding anything contained in any other law for the time being in force, while exercising the	(4) The order referred to in sub-section (2) shall specify the reasons for the inquiry and the scope of the inquiry and may be modified from time to time. (5) Every officer, employee or other person acting under the direct authority of the data fiduciary or the data processor, or a service provider, or a contractor, where services are being obtained by or provided to the data fiduciary or data processor, as the case may be, shall be bound to produce before the Inquiry Officer, all such books, registers, documents, records and any data in their custody or power and to furnish to the Inquiry Officer any statement and information relating to the affairs of the data fiduciary or data processor as the Inquiry Officer may require within such time as the said Inquiry Officer may specify. (6) The Inquiry Officer shall provide a notice in writing to the persons referred to in sub-section (5) stating the reasons thereof and the relationship between the data fiduciary and the scope of inquiry(***). (7) The Inquiry Officer may keep in its custody any books, registers, documents, records and other data produced under sub-section (5) for six months and thereafter shall return the same to the person by whom or on whose behalf such books, registers, documents, records and data are produced, unless an approval to retain such books, registers, documents, record and data for an additional period not exceeding three months has been obtained from the Authority.	

	powers under this section, the Authority or the Inquiry Officer, as the case may be, shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 while trying a suit, in respect of the following matters, namely— *(a)* the discovery and production of books of account, and other documents, at such place and at such time as may be specified; *(b)* summoning and enforcing the attendance of persons and examining them on oath; *(c)* inspection of any book, document, register, record or of any data fiduciary; *(d)* issuing commissions for the examination of witnesses or documents; and *(e)* any other matter which may be prescribed.	(8) Notwithstanding anything contained in any other law for the time being in force, while exercising the powers under this section, the Authority or the Inquiry Officer, as the case may be, shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 while trying a suit, in respect of the following matters, namely— *(a)* the discovery and production of books of account, data and other documents, at such place and at such time as may be specified by regulations; *(b)* summoning and enforcing the attendance of persons and examining them on oath; *(c)* inspection of any book, document, register, record or data of any data fiduciary; *(d)* issuing commissions for the examination of witnesses or documents; and *(e)* any other matter which may be prescribed.	
57.	***Clause 54: Action to be taken by Authority pursuant to an inquiry*** (1) On receipt of a report under sub-section (2) of section 53, the Authority may, after giving such opportunity to the data fiduciary or data processor to make a representation in connection with the report as the Authority deems reasonable, by an order in writing— *(a)* issue a warning to the data fiduciary or data processor where the business or activity is likely to violate the provisions of this Act; *(b)* issue a reprimand to the data fiduciary or data processor where the business or activity has violated the provisions of this Act; *(c)* require the data fiduciary or data processor to cease and desist from committing or causing any violation of the provisions of this Act;	***Clause 54: Action to be taken by Authority pursuant to (***) inquiry*** (1) On receipt of a report under sub-section (2) of section 53, the Authority may, after giving such opportunity to the data fiduciary or data processor to make a representation in connection with the report as the Authority deems reasonable, by an order in writing— *(a)* issue a warning to the data fiduciary or data processor where the business or activity is likely to violate the provisions of this Act; *(b)* issue a reprimand to the data fiduciary or data processor where the business or activity has violated the provisions of this Act;	• The JPC makes cosmetic changes to the marginal heading and certain sub-clauses.

	(d) require the data fiduciary or data processor to modify its business or activity to bring it in compliance with the provisions of this Act; *(e)* temporarily suspend or discontinue business or activity of the data fiduciary or data processor which is in contravention of the provisions of this Act; *(f)* vary, suspend or cancel any registration granted by the Authority in case of a significant data fiduciary; *(g)* suspend or discontinue any cross-border flow of personal data; or *(h)* require the data fiduciary or data processor to take any such action in respect of any matter arising out of the report as the Authority may deems fit. *(2)* A data fiduciary or data processor aggrieved by an order made under this section may prefer an appeal to the Appellate Tribunal.	*(c)* (***) direct the data fiduciary or data processor to cease and desist from committing or causing any violation of the provisions of this Act; *(d)* (***) direct the data fiduciary or data processor to modify its business or activity to bring it in compliance with the provisions of this Act; *(e)* temporarily suspend or discontinue business or activity of the data fiduciary or data processor which is in contravention of the provisions of this Act; *(f)* vary, suspend or cancel any registration granted by the Authority in case of a significant data fiduciary; *(g)* suspend or discontinue any cross-border (***) transfer of personal data; or *(h)* (***) direct the data fiduciary or data processor to take any such action in respect of any matter arising out of the report as the Authority may deem(***) fit. *(3)* A data fiduciary or data processor aggrieved by an order made under this section may prefer an appeal to the Appellate Tribunal under section 73	
58.	***Clause 55: Search and seizure*** (1) Where in the course of inquiry under section 53, the Inquiry Officer has reasonable ground to believe that any books, registers, documents, records or data belonging to any person as mentioned therein, are likely to be tampered with, altered, mutilated, manufactured, falsified or destroyed, the Inquiry Officer may make an application to such designated court, as may be notified by the Central	***Clause 55: Search and seizure*** (1) Where in the course of inquiry under section 53, the Inquiry Officer has reasonable ground to believe that any books, registers, documents, records or data belonging to any person as mentioned therein, are likely to be tampered with, altered, mutilated, manufactured, falsified or destroyed, the Inquiry Officer (***)shall, with the prior approval of the Authority, make an application to such designated court, as may be notified by the Central	• The JPC recommends adding appropriate safeguard to strengthen the Inquiry Officer's power to conduct search and seizure. It adds that an Inquiry Officer must get "prior approval of the Authority" before making an application to the appropriate court for a seizure order. (para 2.209) • The JPC makes certain other cosmetic changes to the clause.

	Government, for an order for the seizure of such books, registers, documents and records. (2) The Inquiry Officer may require the services of any police officer or any officer of any officer of the Central Government, or of both, to assist him for the purposes specified in sub-section (1) and it shall be the duty of every such officer to comply with such requisition. (3) After considering the application and hearing the Inquiry Officer, if necessary, the designated court may, by order, authorise the Inquiry Officer— *(a)* to enter, with such assistance, as may be required, the place or places where such books, registers, documents and records are kept; *(b)* to search that place or those places in the manner specified in the order; and *(c)* to seize books, registers, documents and records it considers necessary for the purposes of the inquiry. (4) The Inquiry Officer shall keep in its custody the books, registers, documents and records seized under this section for such period not later than the conclusion of the inquiry as it considers necessary and thereafter shall return the same to the person, from whose custody or power they were seized and inform the designated court of such return. *(5)* Save as otherwise provided in this section, every search or seizure made under this section shall be carried out in accordance with the provisions of the	Government, for an order for the seizure of such books, registers, documents,(***) records or data. (2) The Inquiry Officer may require the services of any police officer or any officer of the Central Government or State Government, or of (***) all, to assist him for the purposes (***) provided in sub-section (1) and it shall be the duty of every such officer to comply with such requisition. (3) After considering the application and hearing the Inquiry Officer, if necessary, the designated court may, by order, authorise the Inquiry Officer— *(a)* to enter, with such assistance, as may be required, the place or places where such books, registers, documents, (***) records or data are kept; *(b)* to search that place or those places in the manner specified in the order; and *(c)* to seize books, registers, documents, (***) records or data it considers necessary for the purposes of the inquiry. (4) The Inquiry Officer shall keep in (***) his custody the books, registers, documents, (***) records or data seized under this section for such period not later than the conclusion of the inquiry as (***) he considers necessary and thereafter shall return the same to the person, from whose custody or power they were seized and inform the designated court of such return. (5) Save as otherwise provided in this section, every search or seizure made under this section shall be carried out in accordance with the provisions of the	

	Code of Criminal Procedure, 1973 relating to searches or seizures made under that Code.	Code of Criminal Procedure, 1973 relating to searches or seizures made under that Code.	
59.	***Clause 56: co-ordination between authority and other regulators or authorities.*** Where any action proposed to be taken by the Authority under this Act is such that any other regulator or authority constituted under a law made by Parliament or the State legislature may also have concurrent jurisdiction, the Authority shall consult such other regulator or authority before taking such action and may also enter into a memorandum of understanding with such other regulator or authority governing the coordination of such actions.	***Clause 56: co-ordination between authority and other regulators or authorities.*** Where any action proposed to be taken by the Authority under this Act is such that any other regulator or authority constituted under a law made by Parliament or the State legislature may also have concurrent jurisdiction, the Authority shall consult such other regulator or authority before taking such action and may also enter into a memorandum of understanding with such other regulator or authority governing the coordination of such actions including economic activities.	• The JPC notes that actions taken by the DPA under this clause could have economic consequences, requiring further consultation with regulators like the RBI. (para 2.212, 2.213)
	CHAPTER X: PENALTIES AND COMPENSATION		
60.	***Clause 57: Penalties for contravening certain provisions of the Act.*** (1) Where the data fiduciary contravenes any of the following provisions,— *(a)* obligation to take prompt and appropriate action in response to a data security breach under section 25; *(b)* failure to register with the Authority under sub-section (2) of section 26, *(c)* obligation to undertake a data protection impact assessment by a significant data fiduciary under section 27; *(d)* obligation to conduct a data audit by a significant data fiduciary under section 29;	***Clause 57: Penalties for contravening certain provisions of (***) Act*** (1) Where the data fiduciary contravenes any of the following provisions, namely:- *(a)* obligation to take prompt and appropriate action in response to a data (***) breach under section 25; *(b)* failure to register with the Authority under subsection (2) of section 26; *(c)* obligation to undertake a data protection impact assessment by a significant data fiduciary under section 27; *(d)* obligation to conduct a data audit by a significant data fiduciary under section 29; or	• The JPC notes that flexibility in the imposition of penalty is required as digital technologies are rapidly evolving and the quantum of penalty needed to be imposed would need to be decided taking into account these factors. (para 2.215) • The JPC recommends that penalties be imposed as prescribed by the rules, subject to the cap specified in this clause. It retains the reference to 'total worldwide turnover'.

	(e) appointment of a data protection officer by a significant data fiduciary under section 30, it shall be liable to a penalty which may extend to five crore rupees or two per cent. of its total worldwide turnover of the preceding financial year, whichever is higher; (2) Where a data fiduciary contravenes any of the following provisions,— *(a)* processing of personal data in violation of the provisions of Chapter II or Chapter III; *(b)* processing of personal data of children in violation of the provisions of Chapter IV; *(c)* failure to adhere to security safeguards as per section 24; or *(d)* transfer of personal data outside India in violation of the provisions of Chapter VII, it shall be liable to a penalty which may extend to fifteen crore rupees or four per cent. of its total worldwide turnover of the preceding financial year, whichever is higher. (3) For the purposes of this section,— *(a)* the expression "total worldwide turnover" means the gross amount of revenue recognised in the profit and loss account or any other equivalent statement, as applicable, from the sale, supply or distribution of goods or services or on account of services rendered, or both, and where such revenue is generated within India and outside India. *(b)* it is hereby clarified that total worldwide turnover in relation to a data fiduciary is the total worldwide turnover of the data fiduciary and the total worldwide turnover of any group entity of the data fiduciary	*(e)* appointment of a data protection officer by a significant data fiduciary under section 30, it shall be liable to (***) such penalty (***) as may be prescribed, not exceeding, five crore rupees or two per cent. of its total worldwide turnover of the preceding financial year, whichever is higher. (2) Where a data fiduciary contravenes any of the following provisions, namely:— *(a)* processing of personal data in violation of the provisions of Chapter II or Chapter III; *(b)* processing of personal data of children in violation of the provisions of Chapter IV; *(c)* failure to adhere to security safeguards as per section 24; or *(d)* transfer of personal data outside India in violation of the provisions of Chapter VII, it shall be liable to (***) such penalty (***) as may be prescribed (***)as may be prescribed, not exceeding, fifteen crore rupees or four per cent. of its total worldwide turnover of the preceding financial year, whichever is higher. (3)For the purposes of this section,— *(a)* the expression "total worldwide turnover" means the gross amount of revenue recognised in the profit and loss account or any other equivalent statement, as applicable, from the sale, supply or distribution of goods or services or on account of services rendered, or both, and where such revenue is generated within India and outside India.	

	where such turnover of a group entity arises as a result of the processing activities of the data fiduciary, having regard to factors, including— (i) the alignment of the overall economic interests of the data fiduciary and the group entity; (ii) the relationship between the data fiduciary and the group entity specifically in relation to the processing activity undertaken by the data fiduciary; and (iii) the degree of control exercised by the group entity over the data fiduciary or vice versa, as the case may be. *(c)* where of any provisions referred to in this section has been contravened by the State, the maximum penalty shall not exceed five crore rupees under sub-section (1), and fifteen crore rupees under sub-section (2), respectively.	*(b)* it is hereby clarified that total worldwide turnover in relation to a data fiduciary is the total worldwide turnover of the data fiduciary and the total worldwide turnover of any group entity of the data fiduciary where such turnover of a group entity arises as a result of the processing activities of the data fiduciary, having regard to factors, including— (i) (***)activities of the data fiduciary and the group entity are aligned in relation to the processing and use of data; (ii) the exists a relationship between the data fiduciary and the group entity specifically in relation to the processing activity undertaken by the data fiduciary; and (iii) the degree of control exercised by the group entity over the data fiduciary or vice versa, as the case may be. (c)where any of the (***) provisions referred to in this section has been contravened by the State, the maximum penalty shall not exceed five crore rupees under sub-section (1), and fifteen crore rupees under sub-section (2), respectively.	
61.	***Clause 58: Penalty for failure to comply with data principal requests under Chapter V.*** Where, any data fiduciary, without any reasonable explanation, fails to comply with any request made by a data principal under Chapter V, such data fiduciary shall be liable to a penalty of five thousand rupees for each day during which such default continues, subject to a maximum of ten lakh rupees in case of significant data fiduciaries and five lakh rupees in other cases.	***Clause 58: Penalty for failure to comply with data principal requests under Chapter V.*** Where, any data fiduciary, without any reasonable explanation, fails to comply with any request made by a data principal under Chapter V, such data fiduciary shall be liable to a penalty of five thousand rupees for each day during which such default continues, subject to a maximum of ten lakh rupees in case of significant data fiduciaries and five lakh rupees in other cases.	• No change.

62.	***Clause 59: Penalty for failure to furnish report, returns, information, etc.*** If any data fiduciary, who is required under this Act, or the rules or regulations made thereunder, to furnish any report, return or information to the Authority, fails to furnish the same, then such data fiduciary shall be liable to penalty which shall be ten thousand rupees for each day during which such default continues, subject to a maximum of twenty lakh rupees in case of significant data fiduciaries and five lakh rupees in other cases.	***Clause 59: Penalty for failure to furnish report, returns, information, etc.*** If any data fiduciary, who is required under this Act or the rules or regulations made thereunder, to furnish any report, return or information to the Authority, fails to furnish the same, then such data fiduciary shall be liable to a penalty which shall be ten thousand rupees for each day during which such default continues, subject to a maximum of twenty lakh rupees in case of significant data fiduciaries and five lakh rupees in other cases.	• The JPC recommends a cosmetic change.
63.	***Clause 60: Penalty for failure to comply with direction or order issued by Authority.*** If any data fiduciary or data processor fails to comply with any direction issued by the Authority under section 51 or order issued by the Authority under section 54, such data fiduciary or data processor shall be liable to a penalty which may extend to twenty thousand rupees for each day during which such default continues, subject to a maximum of two crores in case of a data processor it may extend to five thousand rupees for each day during which such default continues, subject to a maximum of fifty lakh rupees.	***Clause 60: Penalty for failure to comply with direction or order issued by Authority.*** If any data fiduciary or data processor fails to comply with any directions issued by the Authority under section 51 or order issued by the Authority under section 54,- (i) such data fiduciary (***) shall be liable to a penalty which may extend to twenty thousand rupees for each day during which such default continues, subject to a maximum of two crore rupees(***); or (ii) such data processor shall be liable to a penalty which (***) may extend to five thousand rupees for each day during which such default continues, subject to a maximum of fifty lakh rupees.	• The JPC recommends segregating the penalties stipulated for data fiduciaries and data processors into separate sub-clauses to bring clarity. (para 2.217)
64.	***Clause 61: Penalty for contravention where no separate penalty has been provided.*** Where any person fails to comply with any provision of this Act or the rules or regulations made thereunder applicable to such person, for which no separate penalty	***Clause 61: Penalty for contravention where no separate penalty has been provided.*** Where any person fails to comply with any provision of this Act or the rules or regulations made thereunder applicable to such person, for which no separate penalty	• No change.

	has been provided, then, such person shall be liable to a penalty which may extend to a maximum of one crore rupees in case of significant data fiduciaries, and a maximum of twenty five lakh rupees in other cases.	has been provided, then, such person shall be liable to a penalty which may extend to a maximum of one crore rupees in case of significant data fiduciaries, and a maximum of twenty-five lakh rupees in other cases.	
65.	***No corresponding provision.***	***Clause 62: Right to file complaint or application.*** (1) The aggrieved data principal referred to in section 32 may file a complaint to the Authority within such period and in such manner as may be specified by regulations. (2) The data principal may seek compensation under section 65 by filing an application to the Authority in such form, manner and within such period as may be prescribed. (3) The Authority may forward the complaint or application filed by the data principal to the Adjudicating Officer for adjudging such complaint or application, as the case may be.	• The JPC notes that there is a need for clear language to better allow persons to approach the DPA and to facilitate speedy disposal of cases. (para 2.218) • The JPC observes that Clause 32 and Clause 64 (renumbered as Clause 65) allow a data principal to file a complaint and seek compensation respectively. However, the JPC notes that the procedure to be followed in both cases must be laid down. (para 2.219) • The JPC recommends the creation of a single window system for deciding penalties and compensation when the DPA receives a complaint or application. The JPC further recommends that there must be a "single methodology to decide the course of action" for when the DPA receives a complaint or application. (para 2.219) • To enable this, the JPC inserts a new Clause 62 which states that when DPA receives a complaint or application, it must forward it to the Adjudicating Officer ("**AO**") to be decided. (para 2.219)
66.	***Clause 62: Appointment of Adjudicating Officer.***	***Clause 63: Appointment of Adjudicating Officer.***	• The JPC replaces the word "prescribed" with "required" in Clause 62(1) (renumbered

	(1) For the purpose of adjudging the penalties under sections 57 to 61 or awarding compensation under section 64, the Authority shall appoint such Adjudicating Officer as may be prescribed. (2) The Central Government shall, having regard to the need to ensure the operational segregation, independence, and neutrality of the adjudication under this Act, prescribe— *(a)* number of Adjudicating Officers to be appointed under sub-section (1); *(b)* manner and terms of appointment of Adjudicating Officers ensuring independence of such officers; *(c)* jurisdiction of Adjudicating Officers; *(d)* other such requirements as the Central Government may deem fit. (3) The Adjudicating Officers shall be persons of ability, integrity and standing, and must have specialised knowledge of, and not less than seven years professional experience in the fields of law, cyber and internet laws, information technology law and policy, data protection and related subjects.	(1) For the purpose of adjudging the penalties under sections 57 to 61 or awarding compensation under section 65, the Authority shall appoint such Adjudicating Officers as may be (***) required. (2) The Central Government shall, having regard to the need to ensure the operational segregation, independence, and neutrality of the adjudication under this Act, prescribe— *(a)* the number of Adjudicating Officers to be appointed under sub-section (1); *(b)* the manner and terms of appointment of Adjudicating Officers ensuring independence of such officers; *(c)* the jurisdiction of Adjudicating Officers; and *(d)* such other requirements as (***) may (***) be prescribed. (3) The Adjudicating Officers shall be persons of ability, integrity and standing, and (***) shall possess such qualifications, specialized knowledge, (***) and (***) adequate (***) professional experience, in the fields of law, cyber and internet laws, information technology law and policy, data protection and related subjects, as may be prescribed.	as Clause 63(1)). The JPC also makes cosmetic changes. • The JPC modifies Clause 62(3) (renumbered as Clause 63(3)) to enable the Government to prescribe additional qualifications for the appointment of an Adjudicating Officer, and removes the requirement that the AO must have 7 years' experience.
67.	***Clause 63: Procedure for adjudication by Adjudicating Officer.*** (1) No penalty shall be imposed under this Chapter, except after an inquiry made in such manner as may be prescribed, and the data fiduciary or data processor	***Clause 64: Procedure for adjudication by Adjudicating Officer*** (1) No penalty shall be imposed under this Chapter, except after an inquiry made in such manner as may be prescribed, and the data fiduciary or data	• The JPC omits "reasonable" before the word "opportunity" from Clause 63(1) (renumbered as Clause 64(1)). • The JPC observes that Clause 63(4) of the Bill allows unrestricted power for the AO to decide the quantum of penalty to be imposed

	or any person, as the case may be, has been given a reasonable opportunity of being heard: Provided that no inquiry under this section shall be initiated except by a complaint made by the Authority. (2) While holding an inquiry, the Adjudicating Officer shall have the power to summon and enforce the attendance of any person acquainted with the facts and circumstances of the case to give evidence or to produce any document which, in the opinion of the Adjudicating Officer, may be useful for or relevant to the subject matter of the inquiry. (3) If, on the conclusion of such inquiry, the Adjudicating Officer is satisfied that the person has failed to comply with the provisions of this Act or has caused harm to any data principal as a result of any contravention of the provisions of this Act, the Adjudicating Officer may impose such penalty specified under relevant section. (4) While deciding whether to impose a penalty under sub-section (3) and in determining the quantum of penalty under sections 57 to 61, the Adjudicating Officer shall have due regard to the following factors, namely:— *(a)* nature, gravity and duration of violation taking into account the nature, scope and purpose of processing concerned; *(b)* number of data principals affected, and the level of harm suffered by them; *(c)* intentional or negligent character of the violation; *(d)* nature of personal data impacted by the violation;	processor or any person, as the case may be, has been given an (***) opportunity of being heard: Provided that no inquiry under this section shall be initiated except by a complaint made by the Authority. (2) While holding an inquiry, the Adjudicating Officer shall have the power to summon and enforce the attendance of any person acquainted with the facts and circumstances of the case to give evidence or to produce any document which, in the opinion of the Adjudicating Officer, may be useful for or relevant to the subject matter of the inquiry. (3) If, on the conclusion of such inquiry, the Adjudicating Officer is satisfied that the person has failed to comply with the provisions of this Act or has caused harm to any data principal as a result of any contravention of the provisions of this Act, the Adjudicating Officer may impose such penalty as specified under relevant section. (4) While deciding whether to impose a penalty under subsection (3) and in determining the quantum of penalty under sections 57 to 61, the Adjudicating Officer shall have due regard to the guidelines as may be specified by the Authority for determination and imposition of penalty taking into account any of the following factors, namely:— *(a)* nature, gravity and duration of violation taking into account the nature, scope and purpose of processing concerned;	on a data fiduciary. The JPC recommends restricting this power by requiring the AO to consider the guidelines issued by the DPA while determining and imposing penalty. (para 2.222) • The JPC also makes other cosmetic changes.

	(e) repetitive nature of the default; *(f)* transparency and accountability measures implemented by the data fiduciary or data processor including adherence to any relevant code of practice relating to security safeguards; *(g)* action taken by the data fiduciary or data processor to mitigate the harm suffered by data principals; and *(h)* any other aggravating or mitigating factors relevant to the circumstances of the case, such as, the amount of disproportionate gain or unfair advantage, wherever quantifiable, made as a result of the default. ***(5)*** Any person aggrieved by an order under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal.	*(b)* number of data principals affected, and the level of harm suffered by them; *(c)* intentional or negligent character of the violation; *(d)* nature of personal data impacted by the violation; *(e)* repetitive nature of the default; *(f)* transparency and accountability measures implemented by the data fiduciary or data processor including adherence to any relevant code of practice relating to security safeguards; *(g)* action taken by the data fiduciary or data processor to mitigate the harm suffered by data principals; (***) or *(h)* any other aggravating or mitigating factors relevant to the circumstances of the case, such as, the amount of disproportionate gain or unfair advantage, wherever quantifiable, made as a result of the default. (5) Any person aggrieved by an order made under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal under section 73.	
68.	***Clause 64: Compensation*** (1) Any data principal who has suffered harm as a result of any violation of any provision under this Act or the rules or regulations made thereunder, by a data fiduciary or a data processor, shall have the right to seek compensation from the data fiduciary or the data processor, as the case may be. *Explanation*.—For the removal of doubts, it is hereby clarified that a data processor shall be liable only where it has acted outside or contrary to the instructions of the data fiduciary pursuant to section	***Clause 65: Compensation*** (1) Any data principal who has suffered harm as a result of any violation of any provision under this Act or the rules or regulations made thereunder, by a data fiduciary or a data processor, shall have the right to seek compensation from the data fiduciary or the data processor, as the case may be. *Explanation*.—For the removal of doubts, it is hereby clarified that a data processor shall be liable only where it has acted outside or contrary to the instructions of the data fiduciary pursuant to section	• The JPC observes that the newly inserted Clause 62 providing for the right to file a complaint or application renders Clause 64(2) of the Bill redundant. The JPC accordingly omits it. (para 2.225) • The JPC observes that the words "one complaint" in Clause 64(3) of the Bill are not appropriate to indicate the representative nature of an application on behalf of one or more data principals, or an identifiable class of data principals. Accordingly, the JPC substitutes the words "one complaint" with

	31, or where the data processor is found to have acted in a negligent manner, or where the data processor has not incorporated adequate security safeguards under section 24, or where it has violated any provisions of this Act expressly applicable to it. (2) The data principal may seek compensation under this section by making a complaint to the Adjudicating Officer in such form and manner as may be prescribed. (3) Where there are one or more data principals or any identifiable class of data principals who have suffered harm as a result of any contravention by the same data fiduciary or data processor, one complaint may be instituted on behalf of all such data principals seeking compensation for the harm suffered. (4) While deciding to award compensation and the amount of compensation under this section, the Adjudicating Officer shall have regard to the following factors, namely:— *(a)* nature, duration and extent of violation of the provisions of the Act, rules prescribed, or regulations specified thereunder; *(b)* nature and extent of harm suffered by the data principal; *(c)* intentional or negligent character of the violation; *(d)* transparency and accountability measures implemented by the data fiduciary or the data processor, as the case may be, including adherence to any relevant code of practice relating to security safeguards;	31, or where the data processor is found to have acted in a negligent manner, or where the data processor has not incorporated adequate security safeguards under section 24, or where it has violated any provisions of this Act. (***). (2) (***) (2) Where there are one or more data principals or any identifiable class of data principals who have suffered harm as a result of any contravention by the same data fiduciary or data processor, (***) a representative application may be instituted on behalf of all such data principals seeking compensation for the harm suffered. (3) While deciding to award compensation and the amount of compensation under this section, the Adjudicating Officer shall have regard to any of the following factors, namely:— *(a)* nature, duration and extent of violation of the provisions of the Act, rules (***) or regulations (***) made thereunder; *(b)* nature and extent of harm suffered by the data principal; *(c)* intentional or negligent character of the violation; *(d)* transparency and accountability measures implemented by the data fiduciary or the data processor, as the case may be, including adherence to any relevant code of practice relating to security safeguards; *(e)* action taken by the data fiduciary or the data processor, as the case may be, to mitigate the damage suffered by the data principal;	"representative application" in Clause 64(3) (renumbered as Clause 65(2)). (para 2.226) • The JPC inserts "any of" before the words "following factors" in Clause 64(3) (renumbered as Clause 65(2)). Indicating that the factors are not necessarily to be viewed cumulatively. • The JPC makes cosmetic changes to Clause 64(8) (renumbered as Clause 65(7)) to reflect the procedure of hearing, and other sub-clauses for clarity. (para 2.228)

	(e) action taken by the data fiduciary or the data processor, as the case may be, to mitigate the damage suffered by the data principal; *(f)* previous history of any, or such, violation by the data fiduciary or the data processor, as the case may be; *(g)* whether the arrangement between the data fiduciary and data processor contains adequate transparency and accountability measures to safeguard the personal data being processed by the data processor on behalf of the data fiduciary; *(h)* any other aggravating or mitigating factor relevant to the circumstances of the case, such as, the amount of disproportionate gain or unfair advantage, wherever quantifiable, made as a result of the default. (5) Where more than one data fiduciary or data processor, or both a data fiduciary and a data processor are involved in the same processing activity and are found to have caused harm to the data principal, then, each data fiduciary or data processor may be ordered to pay the entire compensation for the harm to ensure effective and speedy compensation to the data principal. (6) Where a data fiduciary or a data processor has, in accordance with sub-section (5), paid the entire amount of compensation for the harm suffered by the data principal, such data fiduciary or data processor shall be entitled to claim from the other data fiduciaries or data processors, as the case may be, that amount of compensation corresponding to their part of responsibility for the harm caused.	*(f)* previous history of any, or such violation by the data fiduciary or the data processor, as the case may be; *(g)* whether the arrangement between the data fiduciary and data processor contains adequate transparency and accountability measures to safeguard the personal data being processed by the data processor on behalf of the data fiduciary; or *(h)* any other aggravating or mitigating factor relevant to the circumstances of the case, such as, the amount of disproportionate gain or unfair advantage, wherever quantifiable, made as a result of the default. (4) Where more than one data fiduciary or data processor, or both a data fiduciary and a data processor are involved in the same processing activity and are found to have caused harm to the data principal, then, each data fiduciary or data processor may be ordered to pay the entire compensation for the harm to ensure effective and speedy compensation to the data principal. (5) Where a data fiduciary or a data processor has, in accordance with sub-section (4), paid the entire amount of compensation for the harm suffered by the data principal, such data fiduciary or data processor shall be entitled to claim from the other data fiduciaries or data processors, as the case may be, that amount of compensation corresponding to their part of responsibility for the harm caused. (6) Any person aggrieved by an order made under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal under section 73.	

	(7) Any person aggrieved by an order made under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal. (8) The Central Government may prescribe the procedure for hearing of a complaint under this section.	(7) The (***) procedure for hearing of (***) an application under this section shall be such as may be prescribed.	
69.	***Clause 65: Compensation or penalties not to interfere with other punishment.*** No compensation awarded, or penalty imposed, under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under this Act or any other law for the time being in force.	***Clause 66: Compensation or penalties not to interfere with other punishment.*** No compensation awarded, or penalty imposed, under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under this Act or any other law for the time being in force.	• No change.
70.	***Clause 66: Recovery of amounts.*** (1) The amount of any penalty imposed or compensation awarded under this Act, if not paid, may be recovered as if it were an arrear of land revenue. (2) All sums realised by way of penalties under this Act shall be credited to the Consolidated Fund of India.	***Clause 67: Recovery of amounts.*** (1) The amount of any penalty imposed or compensation awarded under this Act, if not paid, may be recovered as if it were an arrear of land revenue. (2) All sums realised by way of penalties under this Act shall be credited to the Consolidated Fund of India.	• No change.
	CHAPTER XI: APPELLATE TRIBUNAL		
71.	***Clause 67: Establishment of Appellate Tribunal*** (1) The Central Government shall, by notification, establish an Appellate Tribunal to—	***Clause 68: Establishment of Appellate Tribunal*** (1) The Central Government shall, by notification, establish an Appellate Tribunal to—	• The JPC notes the Government's suggestion that as the Government is empowered to constitute multiple benches of the Appellate Tribunal in different locations, the number of Members to be appointed to the Appellate Tribunal should be left to its discretion. However, the JPC recommends

	(a) hear and dispose of any appeal from an order of the Adjudicating Officer under sub-section (5) of section 20; *(b)* hear and dispose of any appeal from an order of the Authority under sub-section (2) of section 54; *(c)* hear and dispose of any appeal from an order of the Adjudicating Officer under sub-section (5) of section 63; and *(d)* hear and dispose of any appeal from an order of an Adjudicating Officer under sub-section (7) of section 64. (2) The Appellate Tribunal shall consist of a Chairperson and not more than members to be appointed. (3) The Appellate Tribunal shall be established at such place or places, as the Central Government may, in consultation with the Chairperson of the Appellate Tribunal, notify. (4) Notwithstanding anything contained in sub-sections (1) to (3), where, in the opinion of the Central Government, any existing body is competent to discharge the functions of the Appellate Tribunal under this Act, then, the Central Government may notify such body to act as the Appellate Tribunal under this Act.	*(a)* hear and dispose of any appeal from an order of the Adjudicating Officer under sub-section (5) of section 20; *(b)* hear and dispose of any appeal from an order of the Authority under sub-section (2) of section 54; *(c)* hear and dispose of any appeal from an order of the Adjudicating Officer under sub-section (5) of section 64; and *(d)* hear and dispose of any appeal from an order of an Adjudicating Officer under sub-section (***) (6) of section 65. (2) The Appellate Tribunal shall consist of a Chairperson and (***) such number of members, not exceeding six, to be appointed by the Central Government. (3) The Appellate Tribunal shall be established at such place or places, as the Central Government may, in consultation with the Chairperson of the Appellate Tribunal, notify. (4) Notwithstanding anything contained in sub-sections (1) to (3), where, in the opinion of the Central Government, any existing (***) Tribunal is competent to discharge the functions of the Appellate Tribunal under this Act, then, the Central Government may notify such (***) Tribunal to act as the Appellate Tribunal under this Act.	that the laws should specify the number of members to be appointed. (para 2.233) • The JPC recommends that the Appellate Tribunal must consist of a Chairperson and a maximum of six Members, and modifies Clause 67(2) (renumbered as Clause 68(2)) accordingly. (para 2.233) • The JPC also recommends that the appellate tribunal commences their work no later than twelve months from the date of notification of the Act, although it does not make any changes to the text. (para 1.15.9.6)
72.	***Clause 68: Qualifications, appointment, term, conditions of service of Members.***	***Clause 69: Qualifications, appointment, term, conditions of service of Chairperson and Members.***	• The JPC observes that given the dynamic, technical, and specialized nature of subject matter, and the qualifications that members of global regulators possess, there is a need to include persons with expertise and experience

	(1) A person shall not be qualified for appointment as the Chairperson or a member of the Appellate Tribunal unless he— *(a)* in the case of Chairperson, is, or has been a Judge of the Supreme Court or Chief Justice of a High Court; *(b)* in the case of a member, has held the post of Secretary to the Government of India or any equivalent post in the Central Government for a period of not less than two years or a person who is well versed in the field of data protection, information technology, data management, data science, data security, cyber and internet laws or any related subject. (2) The Central Government may prescribe the manner of appointment, term of office, salaries and allowances, resignation, removal and the other terms and conditions of service of the Chairperson and any member of the Appellate Tribunal.	(1) A person shall not be qualified for appointment as the Chairperson or a Member of the Appellate Tribunal unless he— *(a)* in the case of Chairperson, is , or has been a Judge of the Supreme Court or Chief Justice of a High Court or is qualified to be a Judge of the Supreme Court; *(b)* in the case of a Member, (***) is a person who is (***)an expert and has ability, integrity, standing and specialized knowledge with an experience of not less than twenty years in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, public administration or any related subject. (2) (***) The manner of appointment, term of office, salaries and allowances, resignation, removal and the other terms and conditions of service of the Chairperson and any Member of the Appellate Tribunal, shall be such as may be prescribed.	in fields related to data and privacy as Members of the Appellate Tribunal. (para 2.236) • The JPC notes that it will be beneficial to appoint young persons who are technically qualified. The JPC further observes that such persons may be better in sync with technological innovation, and must be included within the scope of Clause 68 (renumbered as Clause 69)). (para 2.237) • The JPC recommends that the scope of Clause 68(1)(a) (renumbered as Clause 69(1)(a)) should be widened to include persons who would qualify to be appointed as a judge of the Supreme Court under Article 124 of the Constitution of India. The JPC observes that this would allow distinguished jurists and advocates with experience in data protection and information security to be appointed as Chairpersons of the Appellate Tribunal . (para 2.238, 2.239) • The JPC observes that a Secretary to the Government of India or persons in similar posts may not necessarily have the required experience to act as a Member of the Appellate Tribunal . (para 2.240) • The JPC notes that Members' qualifications should emphasize on relevant knowledge, expertise and experience. The JPC recommends the inclusion of these

			factors in Clause 68(1)(b) (renumbered as Clause 69(1)(b)). (para 2.240, 2.241) • The JPC further observes that age should not be a restriction for appointment. (para 2.240) • JPC also inserts "public administration" as a relevant area of experience in Clause 68(1)(b) (renumbered as Clause 69(1)(b)). • The JPC alters the structure of Clause 68(2) (renumbered as Clause 69(2)).
73.	***Clause 69: Vacancies.*** If, for reason other than temporary absence, any vacancy occurs in the office of the Chairperson or a member of the Appellate Tribunal, the Central Government shall appoint another person in accordance with the provisions of this Act and the rules prescribed to fill the vacancy and the proceedings may be continued before the Appellate Tribunal from the stage at which the vacancy is filled.	***Clause 70: Vacancies.*** If, for reason other than temporary absence, any vacancy occurs in the office of the Chairperson or a member of the Appellate Tribunal, the Central Government shall appoint another person in accordance with the provisions of this Act and the rules (***) made thereunder to fill the vacancy and the proceedings may be continued before the Appellate Tribunal from the stage at which the vacancy is filled.	• The JPC proposes cosmetic changes.
74.	***Clause 70: Staff of Appellate Tribunal.*** (1) The Central Government shall provide the Appellate Tribunal with such officers and employees as it may deem fit. (2) The officers and employees of the Appellate Tribunal shall discharge their functions under the general superintendence of its Chairperson.	***Clause 71: Staff of Appellate Tribunal.*** (1) The Central Government shall provide the Appellate Tribunal with such officers and employees as it may deem fit. (2) The officers and employees of the Appellate Tribunal shall discharge their functions under the general superintendence of its Chairperson.	• The JPC inserts the words "payable to" after the word "allowances", and "terms and" before the word "conditions" to bring clarity in Clause 70(3) (renumbered as Clause 71(3)).

	(3) The salaries and allowances and other conditions of service of such officers and employees of the Appellate Tribunal shall be such as may be prescribed.	(3) The salaries and allowances payable to and other terms and conditions of service of such officers and employees of the Appellate Tribunal shall be such as may be prescribed.	
75.	***Clause 71: Distribution of business amongst Benches.*** (1) Subject to the provisions of this Act, the jurisdiction of the Appellate Tribunal may be exercised by Benches thereof, which shall be constituted by the Chairperson. (2) Where Benches of the Appellate Tribunal are constituted under sub-section (1), the Chairperson may, from time to time, by notification, make provisions as to the distribution of the business of the Appellate Tribunal amongst the Benches, transfer of Members between Benches, and also provide for the matters which may be dealt with by each bench. ***(3)*** On the application of any of the parties and after notice to the parties, and after hearing such of them as the Chairperson may desire to be heard, or on the Chairperson's own motion without such notice, the Chairperson of the Appellate Tribunal may transfer any case pending before one Bench, for disposal, to any other Bench.	***Clause 72: Distribution of business amongst Benches.*** (1) Subject to the provisions of this Act, the jurisdiction of the Appellate Tribunal may be exercised by Benches thereof, which shall be constituted by the Chairperson. (2) Where Benches of the Appellate Tribunal are constituted under sub-section (1), the Chairperson may, from time to time, by notification, make provisions as to the distribution of the business of the Appellate Tribunal amongst the Benches, transfer of Members between Benches, and also provide for the matters which may be dealt with by each Bench. (3) On the application of any of the parties and after notice to the parties, and after hearing such of them as the Chairperson may desire to be heard, or on the Chairperson's own motion without such notice, the Chairperson of the Appellate Tribunal may transfer any case pending before one Bench, for disposal, to any other Bench.	• No change.
76.	***Clause 72: Appeals to Appellate Tribunal.*** (1) Any person aggrieved by the decision of the Authority, may prefer an appeal to the Appellate Tribunal within a period of thirty days from the receipt of the order appealed against, in such form, verified in	***Clause 73: Appeals to Appellate Tribunal.*** (1) Any person aggrieved by the decision or order of the Authority or an Adjudicating Officer, may prefer an appeal to the Appellate Tribunal within a period of thirty days from the receipt of the order appealed	• The JPC recommends that an appeal under Clause 72(1) (renumbered as Clause 73(1)) should lie against both a 'decision' as well as an 'order' of the DPA. (para 2.244)

	such manner and be accompanied by such fee, as may be prescribed: Provided that the Appellate Tribunal may entertain any appeal after the expiry of the said period of thirty days if it is satisfied that there was sufficient cause for not filing it within that period. (2) On receipt of an appeal under this section, the Appellate Tribunal may, after providing the parties to the dispute or appeal, an opportunity of being heard, pass such orders thereon as it deems fit. (3) The Appellate Tribunal shall send a copy of every order made by it to the parties to the dispute or the appeal and to the Authority, as the case may be. (4) The Appellate Tribunal may, for the purpose of examining the legality or propriety or correctness, of any decision, or order of the Authority or Adjudicating Officer referred to in the appeal preferred under this section, on its own motion or otherwise, call for the records relevant to disposing of such appeal or application and make such orders as it thinks fit.	against, in such form, verified in such manner and be accompanied by such fee, as may be prescribed: Provided that the Appellate Tribunal may entertain any appeal after the expiry of the said period of thirty days if it is satisfied that there was sufficient cause for not filing it within that period. (2) On receipt of an appeal under this section, the Appellate Tribunal may, after providing the parties to the dispute or appeal, an opportunity of being heard, pass such orders thereon as it deems fit. (3) The Appellate Tribunal shall send a copy of every order made by it to the parties to the dispute or the appeal and to the Authority or the Adjudicating Officer, as the case may be. (4) The Appellate Tribunal may, for the purpose of examining the legality or propriety or correctness, of any decision, or order of the Authority or Adjudicating Officer referred to in the appeal preferred under this section, on its own motion or otherwise, call for the records relevant to disposing of such appeal (***) and make such orders as it thinks fit.	• The JPC also recommends that the right to appeal should be extended to decisions and orders of the AO, and not just that of the DPA. (para 2.244) • The JPC omits the words “or application” after “appeal” from Clause 72(4) of the Bill.
77.	***Clause 73: Procedure and powers of Appellate Tribunal.*** (1) The Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908, but shall be guided by the principles of natural justice and, subject to the other provisions of this Act, the Appellate Tribunal shall have powers to regulate its own procedure.	***Clause 74: Procedure and powers of Appellate Tribunal.*** (1) The Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908, but shall be guided by the principles of natural justice and, subject to the other provisions of this	• The JPC proposes cosmetic changes.

	(2) The Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely— *(a)* summoning and enforcing the attendance of any person and examining his on oath; *(b)* requiring the discovery and production of documents; *(c)* receiving evidence on affidavits; *(d)* subject to the provisions of section 123 and section 124 of the Indian Evidence Act, 1872, requisitioning any public record or document or a copy of such record or document, from any office; *(e)* issuing commissions for the examination of witnesses or documents; *(f)* reviewing its decisions; *(g)* dismissing an application for default or deciding it, *ex parte*; *(h)* setting aside any order of dismissal of any application for default or any order passed by it, *ex parte*; and *(i)* any other matter which may be prescribed.	Act, the Appellate Tribunal shall have powers to regulate its own procedure. (2) The Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely— *(a)* summoning and enforcing the attendance of any person and examining him on oath; *(b)* requiring the discovery and production of documents; *(c)* receiving evidence on affidavits; *(d)* subject to the provisions of sections 123 and (***) 124 of the Indian Evidence Act, 1872, requisitioning any public record or document or a copy of such record or document, from any office; *(e)* issuing commissions for the examination of witnesses or documents; *(f)* reviewing its decisions; *(g)* dismissing an application for default or deciding it *ex parte*; *(h)* setting aside any order of dismissal of any application for default or any order passed by it *ex parte*; and *(i)* any other matter which may be prescribed.	
78.	***Clause 74: Orders passed by Appellate Tribunal to be executable as a decree.*** (1) An order passed by the Appellate Tribunal under this Act shall be executable by the Appellate Tribunal as a decree of civil court, and for this purpose, the	***Clause 75: Orders passed by Appellate Tribunal to be executable as (***) decree.*** (1) (***) Every order (***) made by the Appellate Tribunal under this Act shall be executable by the Appellate Tribunal as a decree of civil court, and for	• The JPC proposes a cosmetic change to the title of the Clause, and other minor changes to Clause 74(1). (para 2.246) • The JPC observes that the Bill already empowers the Appellate Tribunal with the powers of a civil court to execute its orders.

	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.	this purpose, the Appellate Tribunal shall have all the powers of a civil court. (2) (***)	Clause 74(2) in the Bill may dilute the Appellate Tribunal's power to execute its orders by allowing it to transmit its order to a local civil court. This may lead to unnecessary litigation. Accordingly, the JPC omits sub-clause (2) from Clause 74 (renumbered as Clause 75). (para 2.246)
79.	***Clause 75: Appeal to Supreme Court.*** (1) Notwithstanding anything contained in the Code of Civil Procedure, 1908 or in any other law, an appeal shall lie against any order of the Appellate Tribunal, not being an interlocutory order, to the Supreme Court on any substantial question of law. (2) No appeal shall lie against any decision or order made by the Appellate Tribunal with the consent of the parties. (3) Every appeal under this section shall be preferred within a period of ninety days from the date of the decision or order appealed against: Provided that the Supreme Court may entertain the appeal after the expiry of the said period of ninety days, if it is satisfied that the appellant was prevented by sufficient cause from preferring the appeal in time.	***Clause 76: Appeal to Supreme Court.*** (1) Notwithstanding anything contained in the Code of Civil Procedure, 1908 or (***) any other law for the time being in force, an appeal shall lie against any order of the Appellate Tribunal (***) to the Supreme Court on any substantial question of law. (2) (***) (2) Every appeal made under this section shall be preferred within a period of (***) sixty days from the date of the decision or order appealed against: Provided that the Supreme Court may entertain the appeal after the expiry of the said period of (***) sixty days, if it is satisfied that the appellant was prevented by sufficient cause from preferring the appeal in time.	• The JPC observes that Clause 75(2) of the Bill is redundant and omits it. (para 2.248) • The JPC notes that the period of ninety days to make an appeal is excessive, and recommends that it should be reduced to a more appropriate period of sixty days. (para 2.249)
80.	***Clause 76: Right to legal representation.*** The applicant or appellant may either appear in person or authorise one or more legal practitioners or any of its	***Clause 77: Right to legal representation.*** The applicant or appellant may either appear in person or authorize one or more legal practitioners or any of its	• The JPC observes that an applicant or an appellant should have the option to engage domain experts to present their case before the Appellate Tribunal. (para 2.252, 2.253)

	officers to present his or its case before the Appellate Tribunal. *Explanation*.—For the purposes of this section, "legal practitioner" includes an advocate, or an attorney and includes a pleader in practice.	officers or experts to present his or its case before the Appellate Tribunal. *Explanation*.—For the purposes of this section, the expression "legal practitioner" shall include (***) an advocate or an attorney(***).	• The JPC notes that the words "any of its officers" may include domain experts. However, they insert the term "experts" to clarify that such an expert need not be an employee of the applicant or appellant. (para 2.253) • The JPC observes that the word "pleader" is antiquated, and the words "advocate or an attorney" cover the meaning of a legal practitioner. Thus, they omit the words "and includes a pleader in practice" from the Explanation. (para 2.253) • The JPC also proposes cosmetic changes to the Explanation.
81.	***Clause 77: Civil court not to have jurisdiction.*** No civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which the Appellate Tribunal is empowered by or under this Act to determine 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 conferred by or under this Act.	***Clause 78: Civil court not to have jurisdiction.*** No civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which the Appellate Tribunal is empowered by or under this Act to determine 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 conferred by or under this Act.	• No change.
	CHAPTER XII: FINANCE, ACCOUNTS AND AUDIT		
82.	***Clause 78: Grants by Central Government.*** The Central Government may, after due appropriation made by Parliament by law in this behalf, make to the	***Clause 79: Grants by Central Government.*** The Central Government may, after due appropriation made by Parliament by law in this behalf, make to the	• No change.

	Authority grants of such sums of money as it may think fit for the purposes of this Act.	Authority grants of such sums of money as it may think fit for the purposes of this Act.	
83.	***Clause 79: Data Protection Authority of India Funds.*** (1) There shall be constituted a Fund to be called the Data Protection Authority Fund to which the following shall be credited— *(a)* all Government grants, fees and charges received by the Authority under this Act; and *(b)* all sums received by the Authority from such other source as may be decided upon by the Central Government. (2) The Data Protection Authority Fund shall be applied for meeting— (i) the salaries, allowances and other remuneration of the Chairperson, Members, officers, employees, consultants and experts appointed by the Authority; and (ii) the other expenses of the Authority in connection with the discharge of its functions and for the purposes of this Act.	***Clause 80: Data Protection Authority (***) Fund(***).*** (1) There shall be constituted a Fund to be called the Data Protection Authority Fund to which the following shall be credited— *(a)* all Government grants, fees and charges received by the Authority under this Act; and *(b)* all sums received by the Authority from such other source as may be decided upon by the Central Government. (2) The Data Protection Authority Fund shall be applied for meeting— (i) the salaries, allowances and other remuneration of the Chairperson, Members, officers, employees, consultants and experts appointed by the Authority; and (ii) the other expenses of the Authority in connection with the discharge of its functions and for the purposes of this Act.	• The JPC modifies the title of the clause to omit "of India".
84.	***Clause 80: Accounts and Audit.*** (1) The Authority shall maintain proper accounts and other relevant records and prepare an annual statement of accounts in such form as may be prescribed in consultation with the Comptroller and Auditor-General of India.	***Clause 81: Accounts and Audit.*** (1) The Authority shall maintain proper accounts and other relevant records and prepare an annual statement of accounts in such form as may be prescribed in consultation with the Comptroller and Auditor-General of India.	• The JPC modifies Clause 80(4) (renumbered as Clause 81(4)) to clarify that the certified accounts and audit report will be forwarded by the DPA to the Central Government. • The JPC inserts the words "as soon as may be after it is made" after the words "cause the

	(2) The accounts of the Authority shall be audited by the Comptroller and Auditor-General of India at such intervals as may be prescribed and any expenditure incurred by him in connection with such audit shall be reimbursed to him by the Authority. (3) The Comptroller and Auditor-General of India and any other person appointed by him in connection with the audit of the accounts of the Authority shall have the same rights and privileges and authority in connection with such audit as the Comptroller and Auditor-General of India generally has in connection with the audit of the Government accounts and, in particular, shall have the right to demand the production of books, accounts, connected vouchers and other documents and papers, and to inspect any of the offices of the Authority. (4) The accounts of the Authority as certified by the Comptroller and Auditor-General of India or any other person appointed by the Comptroller and Auditor-General of India in this behalf together with the audit report thereon shall be forwarded annually to the Central Government and the Central Government shall cause the same to be laid before each House of the Parliament.	(2) The accounts of the Authority shall be audited by the Comptroller and Auditor-General of India at such intervals as may be prescribed and any expenditure incurred by him in connection with such audit shall be reimbursed to him by the Authority. (3) The Comptroller and Auditor-General of India and any other person appointed by him in connection with the audit of the accounts of the Authority shall have the same rights and privileges and authority in connection with such audit as the Comptroller and Auditor-General of India generally has in connection with the audit of the Government accounts and, in particular, shall have the right to demand the production of books, accounts, connected vouchers and other documents and papers, and to inspect any of the offices of the Authority. (4) The accounts of the Authority as certified by the Comptroller and Auditor-General of India or any other person appointed by (***) him in this behalf together with the audit report thereon shall be forwarded annually to the Central Government by the Authority and the Central Government shall cause the same to be laid, as soon as may be after it is made, before each House of the Parliament.	same to be laid" in Clause 80(4) (renumbered as Clause 81(4)).
85.	***Clause 81: Furnishing of returns, etc., to Central Government.*** (1) The Authority shall furnish to the Central Government at such time and in such form and manner as may be prescribed or as the Central Government may direct, such returns and statements (including statement on	***Clause 82: Furnishing of returns, etc., to Central Government.*** (1) The Authority shall furnish to the Central Government at such time and in such form and manner as may be prescribed or as the Central Government may direct, such returns and statements	• No change.

	enforcement action taken) and such particulars in regard to any proposed or existing programme for the promotion and development of protection of personal data, as the Central Government from time to time, require. (2) The Authority shall prepare once every year in such form and at such time as may be prescribed, an annual report giving a summary of its activities during the previous year and copies of the report shall be forwarded to the Central Government. (3) A copy of the report prepared under sub-section (2) shall be laid, as soon as may be after it is received, before each House of the Parliament. ***(4)*** A copy of the report prepared under sub-section (2) shall also be made publicly available by the Authority.	(including statement on enforcement action taken) and such particulars in regard to any proposed or existing programme for the promotion and development of protection of personal data, as the Central Government from time to time, require. (2) The Authority shall prepare once every year in such form and at such time as may be prescribed, an annual report giving a summary of its activities during the previous year and copies of the report shall be forwarded to the Central Government. (3) A copy of the report prepared under sub-section (2) shall be laid, as soon as may be after it is received, before each House of the Parliament. (4) A copy of the report prepared under sub-section (2) shall also be made publicly available by the Authority.	
CHAPTER XIII: OFFENCES			
86.	***Clause 82: Re-identification and processing of de-identified personal data.*** (1) Any person who, knowingly or intentionally— (a) re-identifies personal data which has been de-identified by a data fiduciary or a data processor, as the case may be; or (b) re-identifies and processes such personal data as mentioned in clause (a), without the consent of such data fiduciary or data processor, then, such person shall be punishable with imprisonment for a term not exceeding	***Clause 83: Re-identification and processing of de-identified personal data.*** (1) Any person who, knowingly or intentionally— (a) re-identifies the personal data which has been de-identified by a data fiduciary or a data processor, as the case may be; or (b) re-identifies and processes such personal data as mentioned in clause (a), without the consent of such data fiduciary or data processor, then, such person shall be punishable with imprisonment for a term not exceeding	• The JPC recommends cosmetic changes.

	three years or with a fine which may extend to two lakh rupees or both. (2) Nothing contained in sub-section (1) shall render any such person liable to any punishment under this section, if he proves that— (a) the personal data belongs to the person charged with the offence under sub-section (1); or (b) the data principal whose personal data is in question has explicitly consented to such re-identification or processing as per the provisions of this Act.	three years or with a fine which may extend to two lakh rupees or with both. (2) Nothing contained in sub-section (1) shall render any such person liable to any punishment under this section, if he proves that— (a) the personal data belongs to the person charged with the offence under sub-section (1); or (b) the data principal whose personal data is in question has explicitly consented to such re-identification or processing as per the provisions of this Act.	
87.	***Clause 83: Offences to be cognizable and non-bailable.*** (1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, an offence punishable under this Act shall be cognizable and non-bailable. (2) No court shall take cognizance of any offence under this Act, save on a complaint made by the Authority.	***Clause 84: Offences to be cognizable and non-bailable.*** (1)Notwithstanding anything contained in the Code of Criminal Procedure, 1973, an offence punishable under this Act shall be cognizable and non-bailable. (2) No court shall take cognizance of any offence punishable under this Act, save on a complaint in writing made by the Authority or by any officer duly authorized by it for this purpose.	• The JPC recommends cosmetic changes and modifies "save on a complaint made by the Authority" in Clause 83(2) (renumbered as 84(2)) to "save on a complaint in writing made by the Authority or by any officer duly authorized by it for this purpose".
88.	***Clause 84: Offences by companies.*** (1) Where an offence under this Act has been committed by a company, every person who, at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.	***Clause 85: Offences by companies*** (1) Where an offence under this Act has been committed by a company, every person who, at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of (***) that part of the business of the company to which the offence relates, as well as the company, (***) shall be liable to be proceeded against and punished accordingly.	• The JPC recognises that an offence may be attributed to a specific part of the business, and not the entire company. Therefore, the words "that part of" were added to Clause 84(1) (renumbered as Clause 85(2)). (para 2.256). So, it would only be officers responsible for that part of the business to which the offence relates, who can be

	(2) Nothing contained in sub-section (1) shall render any such person liable to any punishment provided in this Act, if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence. (3) Notwithstanding anything contained in sub-section (1), where an offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly. *Explanation.*—For the purpose of this section— (*a*) "company" means any body corporate, and includes— (*i*) a firm; and (*ii*) an association of persons or a body of individuals whether incorporated or not. (*b*) "director" in relation to— (*i*) a firm, means a partner in the firm; (*ii*) an association of persons or a body of individuals, means any member controlling affairs thereof.	(2) Nothing contained in sub-section (1) shall render any such person liable to (***) be proceeded against and punished accordingly under this Act, if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence. (3) Notwithstanding anything contained in sub-section (1), where an offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be (***) liable to be proceeded against and punished accordingly**:** Provided that an independent director and a non-executive director of a company shall be held liable only if it is shown that the acts of omission or commission by the company had occurred with his knowledge or with his consent attributable to him or where he had not acted diligently. *Explanation*.— For the purposes of this section, the expressions— (a) "company" means any body corporate, and includes— (i) a firm; and (ii) an association of persons or a body of individuals whether incorporated or not.	penalised, and not all officers responsible for the business generally. • Clause 84(2) (renumbered as 85(2)), states that a person will not be liable to punishment he proves that the offence was committed without his knowledge or he has exercised due diligence to prevent such offence. The JPC recommends that the clause should explicitly mention that the person shall be free from all "proceedings" and "punishment" once he proves that the offence was committed without his knowledge and that he exercised all due diligence. (para 2.256) • The JPC notes that Clause 84 (renumbered as Clause 85), does not include any provision for liability of independent directors or a non-executive director of a company. Therefore, the JPC inserts proviso to Clause 85(3) which attributes liability to an independent or non-executive director only if it is shown that acts of omission or commission by the company had occurred with his knowledge or consent, or where he had not acted diligently. (para 2.257) • The JPC recommends other cosmetic changes.
89.	***Clause 85: Offences by State.***	***Clause 86: Offences by (***) Government data fiduciaries***	• The JPC notes the submission of the MEITY, on 18.12.2020, that the state is a sovereign entity and may not be directly

	(*1*) Where it has been proved that an offence under this Act has been committed by any department or authority or body of the State, by whatever name called, the head of such department or authority or body shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly. (*2*) Nothing contained in sub-section (*1*) shall render any such person liable to any punishment provided in this Act, if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence. (*3*) Notwithstanding anything contained in sub-section (*1*), where an offence under this Act has been committed by a department of the Central or State Government, or any authority of the State and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of, any officer, other than the head of the department or authority, such officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly. (4) Notwithstanding anything in this section, the provisions of the Code of Criminal Procedure, 1973 relating to public servants shall continue to apply.	(1) Where (***) an offence under this Act has been committed by any (***) Government data fiduciary, an in- house enquiry shall be conducted by the Head of Office of the concerned data fiduciary and the person or officer concerned responsible for such offence shall be liable to be proceeded against and punished accordingly. (2) Nothing contained in sub-section (1) shall render any such person or officer liable to any punishment provided in this Act, if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence (3) Notwithstanding anything contained in sub-section (1), where an offence under this Act has been committed by a (***) Government data fiduciary and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of, any officer, other than the (***) person or officer concerned referred to in sub-section (1), such officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly. (4)Notwithstanding anything contained in this section, the provisions of the Code of Criminal Procedure, 1973 relating to public servants shall continue to apply.	indicated as responsible for any offence. Therefore, the marginal heading to Clause 85 (renumbered as Clause 86), be amended and now read as "Offences by Government data fiduciaries". (para 2.260, 2.261) • The JPC also suggests changes to sub-clause (1)- such that it is not the head of a department who would be guilty of the offence. In the JPC's view, if the HOD is held guilty, that would impede the functioning of the department and create hurdles in everyday functioning. The JPC recommends that the HOD must first conduct an in-house inquiry to determine the officer responsible for the offence. The liability should be decided subsequently. (para 2.2.62) • The JPC observes that since the Government will be a "significant data fiduciary, it will have to establish Standard Operating Procedures in the Ministries and Departments etc. to protect the huge amount of data that is collected, although it does not suggest any text changes to this effect. (para 2.262)
CHAPTER XIV: MISCELLANEOUS			

90.	***Clause 86: Power of central government to issue directions***. (1) The Central Government may, from time to time, issue to the Authority such directions as it may think necessary in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order (2) Without prejudice to the foregoing provisions of this Act, the Authority shall, in exercise of its powers or the performance of its functions under this Act, be bound by such directions on questions of policy as the Central Government may give in writing to it from time to time: Provided that the Authority shall, as far as practicable, be given an opportunity to express its views before any direction is given under this sub-section. (3) The decision of the Central Government whether a question is one of policy or not shall be final.	***Clause 87: Power of central government to issue directions*** (1) The Central Government may, from time to time, issue to the Authority such directions as it may think necessary in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order. (2) Without prejudice to the foregoing provisions of this Act, the Authority shall, in exercise of its powers or the performance of its functions under this Act, be bound by such directions (***) as the Central Government may give in writing to it from time to time: Provided that the Authority shall, as far as practicable, be given an opportunity to express its views before any direction is given under this sub-section. (3) (***)	• The JPC finds that the Central Government has been empowered, under Clause 86 (renumbered as Clause 87), to issue directions to the DPA only on questions of policy, and that the DPA is bound by the directions of the Central Government only on questions of policy. (para 2.266) • The JPC recommends that the DPA should be bound by the directions of the Central Government in all cases and not just on questions of policy. As a result, the words "on questions of policy" have been removed. The JPC notes that this means the decision of the Central Government is final in every case, and makes Clause 86(3), (renumbered Clause 87(3)), superfluous and, therefore, it has been deleted in its entirety. (para 2.266)
91.	***Clause 87: Members, etc., to be public servants.*** The Chairperson, Members, officers and employees of the Authority and the Appellate Tribunal shall be deemed, when acting or purporting to act in pursuance of any of the provisions of this Act, to be public servants within the meaning of section 21 of the Indian Penal Code.	***Clause 88: Members, etc., to be public servants.*** The Chairperson, Members, officers and employees of the Authority and the Appellate Tribunal shall be deemed, when acting or purporting to act in pursuance of any of the provisions of this Act, to be public servants within the meaning of section 21 of the Indian Penal Code.	• No change.

92.	***Clause 88: Protection of action taken in good faith.*** No suit, prosecution or other legal proceedings shall lie against the Authority or its Chairperson, member, employee or officer for anything which is done in good faith or intended to be done under this Act, or the rules prescribed, or the regulations specified thereunder.	***Clause 89: Protection of action taken in good faith.*** No suit, prosecution or other legal proceedings shall lie against the Authority or its Chairperson, Member, employee or officer for anything which is (***) in good faith done or intended to be done under this Act, or the rules (***) or (***) regulations (***) made thereunder.	• The JPC has made cosmetic changes.
93.	***Clause 89: Exemption from tax on income.*** Notwithstanding anything contained in the Income Tax Act, 1961 (43 of 1961) or any other enactment for the time being in force relating to tax on income, profits or gains, as the case may be, the Authority shall not be liable to pay income tax or any other tax in respect of its income, profits or gains derived.	***Clause 90: Exemption from tax on income.*** Notwithstanding anything contained in the Income Tax Act, 1961 or any other enactment for the time being in force relating to tax on income, profits or gains, as the case may be, the Authority shall not be liable to pay income tax or any other tax in respect of its income, profits or gains derived.	• No change.
94.	***Clause 90: Delegation.*** The Authority may, by general or special order in writing delegate to any member or officer of the Authority subject to such conditions, if any, as may be specified in the order, such of its powers and functions under this Act, except the powers under section 94, as it may deem necessary.	***Clause 91: Delegation*** The Authority may, by general or special order in writing delegate to any Member or officer of the Authority subject to such conditions, if any, as may be specified in the order, such of its powers and functions under this Act, except the powers to make regulations under section 95, as it may deem necessary.	• The JPC has recommended cosmetic changes.
95.	***Clause 91: Act to promote framing of policies for digital economy, etc.*** (1) Nothing in this Act shall prevent the Central Government from framing of any policy for the digital economy, including measures for its growth, security,	***Clause 92: Act to promote framing of policies for digital economy, etc.*** (1) Nothing in this Act shall prevent the Central Government from framing (***) any policy for the digital economy, including measures for its growth,	• The JPC observes that sub-clause (1) does not refer to policies for non-personal data. It therefore recommends removing the phrase 'insofar as such policy do not govern personal data". And recommends adding "handling of non-personal data including anonymised

	integrity, prevention of misuse, insofar as such policy do not govern personal data. (2) The Central Government may, in consultation with the Authority, direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed. Explanation.—For the purposes of this sub-section, the expression "non-personal data" means the data other than personal data. (3) The Central Government shall disclose annually the directions, made by it under sub-section (2), in such form as may be prescribed	security, integrity, prevention of misuse, **(***)** and handling of non-personal data including anonymised personal data. (2) The Central Government may, in consultation with the Authority, direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulation of evidence- based policies by the Central Government, in such manner as may be prescribed. *Explanation*.-(***) (3) The Central Government shall disclose annually the directions, made by it under sub-section (2), in such form as may be prescribed and such disclosure shall be included in its Annual Report which shall be laid before each House of Parliament.	personal data". (para 2.271). So, the Central Government can make any policies for the digital economy, including on handling of NPD. • The JPC recommends deleting the definition of NPD in the explanation- since it is added to the definitions clause (para 2.272) • The JPC notes that since the Bill already has provisions for rules, regulations, orders and notifications including the Annual report of the DPA to be laid before the Parliament, the directions issued from time to time under Clause 91(2) (renumbered Clause 92(2)), may also be put forth before the Parliament in the form of a report to be placed annually before both the Houses. This will ensure greater accountability of the executive towards the legislature with respect to the directions under this Bill. (para 2.273)
96.	***Clause 92: Bar on processing certain forms of biometric data.*** No data fiduciary shall process such biometric data as may be notified by the Central Government, unless such processing is permitted by law.	***Clause 93: Bar on processing certain forms of biometric data.*** (***) Any data fiduciary shall not process such biometric data as may be (***) prescribed, unless such processing is permitted by law.	• The JPC suggests that the word 'notified' be replaced with 'prescribed'. Meaning that the government will prescribe rules for this purpose, and not notifications.
97.	***Clause 93: Power to make rules.*** (1) The Central Government may, by notification, make rules to carry out the purposes of this Act.	***Clause 94: Power to make rules.***	• The JPC, on account of the changes made to the substantive provisions in the Bill from Clause 1 to 92 suggests consequential

	(2) In particular, 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) any other categories of sensitive personal data under section 15; (b) other factors to be taken into consideration under clause (d) of sub-section (3) of section 16; (c) the form and manner in which an application may be made to exercise the right under sub-section (2), and the manner of review of the order passed by the Adjudicating Officer under sub-section (4) of section 20; (d) the methods of voluntary identification to identify users of social media under sub-section (3) and the identifying mark of verification of a voluntarily verified user under sub-section (4) of section 28; (e) the manner in which a complaint may be filed under sub-section (4) of section 32; (f) the entity or class of entity in a country, or international organisations to which transfers may be permitted under clause (b) of sub-section (1) of section 34; (g) the place of head office of the Authority under sub-section (3) of section 41; (h) procedure to be followed by the selection committee under sub-section (3) of section 42; (i) the salaries and allowances payable to, and other terms and conditions of service of the Chairperson and the Members of the Authority under sub-section (2) of section 43; (j) the time and place for, and the rules and procedures in regard to, transaction of business at the meetings of the Authority under sub-section (1) of section 46;	(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) (***) any other harm under sub-clause (xii) of clause (23) of section 2; (b) the manner in which a data fiduciary can share, transfer or transmit the personal data to any person as part of any business transaction under sub-section (4) of section 8; (c) the other factors to be taken into consideration under clause (d) of sub-section (3) of section 16; (d) the form and manner in which an application may be made to exercise the right under sub-section (2), and the manner of review of the order passed by the Adjudicating Officer under sub-section (4) of section 20; (e) the steps to be taken by the Authority in case of breach of non-personal data under sub-section (6) of section 25; (f) the threshold with respect to users of social media platform under sub-clause (i) of clause (f) of sub-section (1) and different thresholds for different classes of social media platforms under the proviso to clause (f) of sub- section (1) of section 26; (g) the (***) manner of voluntary (***) verification of the accounts of the users of social media platform under sub-section (3) and the identifying mark of verification of a voluntarily verified user under sub-section (4) of section 28;	changes in the rule-making power of the Central Government. • These include adding rule-making powers for breach of non-personal data, deciding the penalties for contraventions of certain provisions of the Bill, among others.

	(k) other functions of the Authority under clause (o) of sub-section (2) of section 49; (l) the procedure of issuance of a code of practice under sub-section (4), the manner in which the Authority may review, modify or revoke a code of practice under sub-section (7), of section 50; (m) other matters under clause (e) of sub-section (8) of section 53, in respect of which the Authority shall have powers; (n) the number of Adjudicating Officers, manner and terms of their appointment, their jurisdiction and other requirements under sub-section (2) of section 62; (o) the manner in which the Adjudicating Officer shall conduct an inquiry under sub-section (1) of section 63; (p) the form and manner of making a complaint under sub-section (2), and the procedure for hearing of a complaint under sub-section (8) of section 64; (q) the manner of appointment, term of office, salaries and allowances, resignation, removal and the other terms and conditions of service of the Chairperson and any member of the Appellate Tribunal under sub-section (2) of section 68; (r) the procedure of filling of vacancies in the Appellate Tribunal under section 69; (s) the salaries and allowances and other conditions of service of the officers and employees of the Appellate Tribunal under sub-section (3) of section 70; (t) the form, manner and fee for filing an appeal or application, as the case may be, with the Appellate Tribunal under sub-section (1) of section 72; (u) other matters under clause (i) of sub-section (2) of section 73 in respect of powers of the Appellate Tribunal; (v) the form of accounts, other relevant records and annual statement of accounts under sub-section (1), the	(h) (***) the manner of registration of data auditors under sub-section (4) of section 29; (i) the qualifications and experience of data protection officer and other personnel to be included under the expression "key managerial personnel" under sub-section (1) of section 30; (j) the entity or class of (***) entities in a country, or international organisations to which transfers may be permitted under clause (b) of sub-section (1) of section 34; (k) the place of head office of the Authority under sub-section (3) of section 41; (l) the procedure to be followed by the selection committee under sub-section (3) of section 42; (m) the salaries and allowances payable to, and other terms and conditions of service of the Chairperson and the Members of the Authority under sub-section (2) of section 43; (n) the time and place for, and the rules and procedures in regard to transaction of business at the meetings (including quorum) of the Authority under sub-section (1) of section 46; (o) other functions of the Authority under clause (p) of sub-section (2) of section 49; (p) the procedure of issuance of a code of practice under sub-section (4), the manner in which the Authority may review, modify or revoke a code of practice under sub-section (7), of section 50; (q) other matters under clause (e) of sub-section (8) of section 53 in respect of which the Authority shall have powers; (r) the penalties for contravening of certain provisions of this Act by data fiduciaries including by State under sub-sections (1), (2) and (3) of section 57;	

	intervals at which the accounts of the Authority shall be audited under sub-section (2) of section 80; (w)the time in which and the form and manner in which the returns, statements, and particulars are to be furnished to the Central Government under sub-section (1), and annual report under sub-section (2) of section 81; (x) the manner in which the Central Government may issue a direction, including the specific purposes for which data is sought under sub-section (2) and the form of disclosure of such directions under sub-section (3) of section 91; or (y) any other matter which is require to be, or may be, prescribed, or in respect of which provision is to be made, by rules.	(s) the form, manner and the period for filing an application for compensation under sub-section (2) of section 62; (t) the number of Adjudicating Officers, manner and terms of their appointment, their jurisdiction and other requirements under sub-section (2) and the qualifications and the experience of such Adjudicating Officers under sub-section (3) of section 63; (u) the manner in which the Adjudicating Officer shall conduct an inquiry under sub-section (1) of section 64; (v) the form and manner of making an application (***) and the procedure for hearing of (***) an application under sub-section (7) of section 65; (w) the manner of appointment, term of office, salaries and allowances, resignation, removal and the other terms and conditions of service of the Chairperson and any Member of the Appellate Tribunal under sub-section (2) of section 69; (x) the procedure of filling of vacancies in the Appellate Tribunal under section 70; (y) the salaries and allowances and other conditions of service of the officers and employees of the Appellate Tribunal under sub-section (3) of section 71; (z) the form, manner and fee for filing an appeal (***) with the Appellate Tribunal under sub-section (1) of section 73; (za) other matters under clause (i) of sub-section (2) of section 74 in respect of powers of the Appellate Tribunal; (zb) the form of accounts, other relevant records and annual statement of accounts under sub-section (1), the intervals at which the accounts of the Authority shall be audited under sub-section (2) of section 81; (zc) the time, (***) the form and manner in which the returns, statements, and particulars are to be furnished	

		to the Central Government under sub-section (1), and annual report under sub-section (2) of section 82; (zd) the manner in which the Central Government may issue a direction, including the specific purposes for which data is sought under sub-section (2) and the form of disclosure of such directions under sub-section (3) of section 92; (ze) the details of biometric data not to be processed under section 93; (zf) any other matter which is required to be, or may be prescribed, or in respect of which provision is to be made, by rules.	
98.	***Clause 94: Power to make regulations.*** (1) The Authority may, by notification, make regulations consistent with this Act and the rules made thereunder to carry out the provisions of this Act. (2) In particular and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:— (a) information required to be provided by the data fiduciary to the data principal in its notice under clause (n) of sub-section (1) of section 7; (b) manner in which the personal data retained by the data fiduciary must be deleted under sub-section (4) of section 9; (c) the safeguards for protecting the rights of data principals under sub-section (3) of section 14; (d) the additional safeguards or restrictions under sub-section (2) of section 15; (e) the manner of obtaining consent of the parent or guardian of a child under sub-section (2), the manner	***Clause 95: Power to make regulations.*** (1) The Authority may, by notification and subject to the condition of previous publication, make regulations, not inconsistent with the provisions of this Act and the rules made thereunder, to carry out the (***) purposes of this Act. (2) In particular and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:— (a) any other information required to be provided by the data fiduciary to the data principal in its notice under clause (n) of sub-section (1) of section 7; (b) the manner in which the personal data retained by the data fiduciary must be deleted under sub-section (4) of section 9; (c) the reasonable purposes under sub-section (1) and the safeguards for protecting the rights of data principals under sub-section (3) of section 14;	• The JPC, on account of the changes made to the substantive provisions in the Bill from Clause 1 to 92 recommends consequential changes in the regulation-making power of the Central Government as provided under Clause 94 (renumbered as Clause 95).

	of verification of age of a child under sub-section (3), application of provision in modified form to data fiduciaries offering counselling or child protection services under sub-section (6) of section 16; (f) the period within which a data fiduciary must acknowledge the receipt of request under sub-section (1), the fee to be charged under sub-section (2), the period within which request is to be complied with under sub-section (3), and the manner and the period within which a data principal may file a complaint under sub-section (4) of section 21; (g) the manner for submission of privacy by design policy under sub-section (2) of section 22; (h) the manner and the technical, operation, financial and other conditions for registration of the consent manager and its compliance under sub-section (5) of section 23; (i) the manner of registration of significant data fiduciaries under sub-section (2) of section 26; (j) the circumstances or classes of data fiduciaries or processing operations where data protection impact assessments shall be mandatory and instances where data auditor shall be appointed under sub-section (2), and the manner in which data protection officer shall review the data protection impact assessment and submit to the Authority under sub-section (4) of section 27; (k) the form and manner for maintaining the records, and any other aspect of processing for which records shall be maintained under sub-section (1) of section 28; (l) the other factors to be taken into consideration under clause (g) of sub-section (2); the form and procedure for conducting audits under sub-section (3); the manner of registration of auditors under sub-section (4); criteria on the basis of which rating in the form of	(d) the additional safeguards or restrictions under sub-section (2) of section 15; (e) the manner of obtaining consent of the parent or guardian of a child (***) and the manner of verification of age of a child under sub-section (2), application of provision in modified form to data fiduciaries offering counselling or child protection services under sub-section (5) of section 16; (f) the manner in which the data principal shall have the right to access in one place the identities of the data fiduciaries with whom his personal data has been shared by any data fiduciary together with the categories of personal data shared with them under sub-section (3) of section 17; (g) the conditions and the manner in which the data principal shall have the right to correction and erasure of the personal data under section 18; (h) the manner for determining the compliance which would not be technically feasible for non- application of the provisions of sub-section (1) under clause (b) of sub-section (2) of section 19; (i) the period within which a data fiduciary must acknowledge the receipt of request under sub-section (1), the fee to be charged under sub-section (2), the period within which request is to be complied with under sub-section (3), and the manner and the period within which a data principal may file a complaint under sub-section (4) of section 21; (j) the conditions under which the data fiduciary shall oblige to comply with the request made by the data principal under sub-section (5) of section 21; (k) the manner and the period for submission of privacy by design policy under sub-section (2) of section 22; (l) the form and manner for making the information available, any other information to be maintained by the	

	a data trust score may be assigned to a data fiduciary under sub-section (6) of section 29; (m) the qualification and experience of a data protection officer under sub-section (1) of section 30; (n) the period within which transfer of personal data shall be notified to the Authority under sub-section (3) of section 34; (o) the provisions of the Act and the class of research, archival or statistical purposes which may be exempted under section 38; (p) the remuneration, salary or allowances and other terms and conditions of service of such officers, employees, consultants and experts under sub-section (2) of section 48; (q) the code of practice under sub-section (1) of section 50; (r) the form and manner for providing information to the Authority by the data fiduciary under sub-section (3) of section 52; (s) any other matter which is required to be, or may be specified, or in respect of which provision is to be or may be made by regulations.	data fiduciary under sub-section (1) and the manner of notifying the important operations in the processing of personal data related to data principal under sub-section (2) of section 23; (m) the manner and the technical, operational, financial and other conditions for registration of the Consent Manager (***) under sub-section (5) of section 23; (n) the manner of review of security safeguards periodically by data fiduciary or data processor under sub-section (2) of section 24; (o) the form of notice under sub-section (2) of section 25; (p) the manner of registration of significant data fiduciaries under sub-section (2) of section 26; (q) the circumstances or class (***) of data fiduciaries or processing operations where data protection impact assessments shall be mandatory and instances where data auditor shall be (***) engaged under sub-section (2), (***) the manner in which data protection officer shall review the data protection impact assessment and submit to the Authority under sub-section (4) of section 27(***) and the conditions for processing under sub-section (5) of section 27; (r) the form and manner for maintaining the records, and any other aspect of processing for which records shall be maintained under sub-section (1) of section 28; (s) the other factors to be taken into consideration under clause (g) of sub-section (2); the form and procedure for conducting audits under sub-section (3); (***) criteria on the basis of which rating in the form of a data trust score may be assigned to a data fiduciary under sub-section (6) of section 29; (t) the period within which transfer of personal data shall be notified to the Authority under sub-section (3) of section 34;	

		(u) the provisions of the Act and the class of research, archiving or statistical purposes which may be exempted under section 38; (v) the manner of inclusion by the data fiduciary for inclusion in the Sandbox under sub-section (2) and any other information required to be included in the Sandbox by the data fiduciary under clause (d) of sub-section (3) of section 40; (w) the remuneration, salary or allowances and other terms and conditions of service of such officers, employees, consultants and experts under sub-section (2) of section 48; (x) the code of practice under sub-section (1) of section 50; (y) the manner, period and form (***) for providing information to the Authority by the data fiduciary or data processor under sub-section (3) of section 52; (z) the place and time for discovery and production of books of account, data and other documents to the Authority or Inquiry Officer under clause (a) of sub-section (8) of section 53; (za) the period and the manner of filing a complaint by the data principal before the Authority under sub-section (1) of section 62; (zb) any other matter which is required to be, or may be specified, or in respect of which provision is to be or may be made by regulations.	
99.	***Clause 95: Rules and regulations to be laid before Parliament.*** Every rule and regulation made under this Act and notification issued under sub-section (4) of section 67 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	***Clause 96: Rules and regulations to be laid before Parliament.*** Every rule and regulation made under this Act and notification issued under sub-section (4) of section 68 shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a	• The JPC has recommended a cosmetic change.

	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 regulation or notification or both Houses agree that the rule or regulation or notification should not be made, the rule or regulation 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 regulation or notification.	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 regulation or notification or both Houses agree that the rule or regulation or notification should not be made, the rule or regulation 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 regulation or notification.	
100.	***Clause 96: Overriding effect of this Act.*** Save as otherwise provided in this Act, the provisions of this Act shall have effect notwithstanding anything inconsistent therewith any other law for the time being in force or any instrument having effect by virtue of any law other than this Act.	***Clause 97: Overriding effect of this Act.*** Save as otherwise provided in this Act, the provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force or any instrument having effect by virtue of any such law (***).	• The JPC has recommended cosmetic changes.
101.	***Clause 97: Power to remove difficulties.*** (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 be necessary or expedient for removing the difficulty: Provided that no such order shall be made	***Clause 98: Power to remove difficulties.*** (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: Provided that no such order	• The JPC has recommended cosmetic changes.

	under this section after the expiry of five years from the commencement of this Act. (2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.	shall be made under this section after the expiry of five years from the date of commencement of this Act. (2)Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.	
102.	***Clause 98: Amendment of Act 21 of 2000.*** The Information Technology Act, 2000 shall be amended in the manner specified in the Schedule to this Act.	***Clause 99: Amendment of Act 21 of 2000.*** The Information Technology Act, 2000 shall be amended in the manner specified in the Schedule to this Act.	• No change.