Foundation of Data Protection Professionals in India
[Not for Profit, Section 8 Company limited by guarantees: CIN No: U72501KA2018NPL116325]
Registered Office: No 37, "Ujvala", 20th Main, BSK first Stage, Second Block, Bangalore 560050
Web: www.fdppi.in: E Mail fdppi@fdppi.in: Ph: 08026603490: Mob: +91 8310314516

6th September 2020

To

The JCPDPB Cell

Loksabha Secretariat

New Delhi

Dear Sir,

With reference to your e-mail of 28th August 2020, we are enclosing herewith our recommendation on section wise modifications to Personal Data Protection Bill 2019 as per the suggested format.

We hope this would be of use.

In case any further clarification is required, we will be happy to provide the same.

Thanking you

Yours sincerely

Vijayashankar Nagarajarao Shankaranarayanappa

Digitally signed by Vijayashankar Nagarajarao Shankaranarayanappa
DN: c=IN, o=Personal, title=5824, pseudonym=d13cc10c4ef1030c0b205f8598edde797a00c1d4, 2.5.4.20=4cafa42b450c62d6713de56c944d7ac0175f34ccc8733807b5efdc2a6e947975, postalCode=560050, st=Karnataka, serialNumber=b4b30b619771293be8f3a37a5679bbfa3c21daa73d6c684df9326da3e8cca118, cn=Vijayashankar Nagarajarao Shankaranarayanappa
Date: 2020.09.07 09:27:14 +05'30'

Na.Vijayashankar
Chairman

Section wise recommendations on Personal Data Protection Bill 2019

FORMAT FOR SUBMISSION OF PROPOSED AMENDMENTS ON THE PROVISIONS OF THE PDP BILL 2019

	Sec	**Text of Section/Clause of the Bill**	***Key Concerns of the Sections/Clause***	**Text of the proposed Amendments**
1	1(2)	It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint; and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision.	*Currently no date has been indicated for the different aspects of the act to become effective.* *Some of the other countries provided a lead time for the published act to become effective and some have provided for deferment of the enforcement by around 6 months from the date the legislation became effective.* *In PDPB iIt is mandatory to appoint the DPA within 3 months. Subsequently the implementation will be decided by the DPA.* *If no date of implementation is defined in the Act, there could be complacency in issuing further regulatory guidelines by DPA and enforcing the Act.*	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 giving effect to different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision. **Provided further that, the act in its entirety shall be effective at the end of 12 months from the date of notification of the Act.**

			Hence a time line is required to be indicated. *Uncertainty would also be creating problems for the industry on handling legacy data collected till the date of notification.* *Hence it is suggested that the outer limit may be set as 12 months. PDPA 2018 had indicated 18 months and there is already more than 18 months delay from the day PDPA 2018 was published. A further delay of more than 12 months would not be desirable.* *DPA can always delay the enforcement fines if there is a further need.*	
2	3(27)	"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;	*This definition of person is with reference to the Data fiduciary or Data Processor.* *Person is also used in conjunction with "Natural" to define the applicability of the Act from the perspective of a data principal.* *The confusion may be removed by a small change as suggested.*	**"Person" in the context of a "data principal" means an individual and <u>in the context of business as Data Fiduciary or Data Processor</u>** 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;
3	3(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;	*1.The act is meant to protect the Privacy of Indian Citizens as per the constitutional requirement.* *Also, the protection is dependent on the "Consent" which is a "contract" which extinguishes automatically on the death of the individual.* *Hence a dead person cannot provide a valid consent and there is no constitutional right of Privacy.* *Hence the law is not applicable for a deceased person and this needs to be clarified.* *2.Personal data often includes a category of data which has the characteristics of name or number but relates to a business entity and not a living natural person.* *In Singapore law this is specifically mentioned as "Business Data" and excluded from Personal data.*	"Personal data" means data about or relating to a **living** 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; **but excludes any data used for identifying a business or used for business communication or business purpose in the name of any juridical entity**

			Some EU Countries define even proprietary concerns as personal data. *In India we have HUF entities which may also be business entities.* *To consider information in respect of Proprietary concerns and HUF as "Personal Data" may be undesirable* *This could create an unnecessarily burden to small enterprises who carry on business in proprietary HUF or partnership names which reflect personal names of the owners.* *Hence the personal data definition should exclude business data.*	
4	3(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;	*1.The credentials used for access of any computer system such as the OTP or Password has not been included in the list of sensitive information.* *There is a need to secure such data with a higher level of security than other information.* *Hence it should be added to the list of Sensitive personal information as is*	"Sensitive personal data" means such personal data, which may, reveal, be related to, or constitute— **(i) Password, or any means used as credentials of a person to access data residing inside a computer resource** (ii) financial data; (iii) health data; (iv) official identifier; (v) sex life; (vi) sexual orientation;

		(xi) religious or political belief or affiliation; or (xii) any other data categorized as sensitive personal data under section 15.	*currently prevailing under Section 43A of ITA 2000.* *2.The inclusion of Caste, Tribe, Religious or Political beliefs are practically impossible to be segregated from non-sensitive data since "Name" is often indicative of religion and caste and "belief" is an interpretation of content.* *It is suggested they are removed from the list. If necessary, they can be added through regulations since what is of concern is profiling based on caste or political or religious beliefs and not the mere collection of the information.*	(vii) biometric data; (viii) genetic data; (ix) transgender status; (x) intersex status; (xi) any other data categorized as sensitive personal data under section 15.;
5	3 (xx)	**Additional**	*The definition of Personal data and Data Principal refers to a single individual.* *However when personal data is generated in a transaction between two or more individuals, the rights on the personal data should be recognized for all such persons.* *This was referred to as "Community Data" by the Srikrishna Committee but not included in the Act.*	**(xx)"Joint personal Data" means any data about or related to more than one living natural person/s who may be directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural persons, 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**

			It was left to be covered by the Non Personal Data (NPD) Governance regulation which is now under consideration . *But NPD regulation does not deal with "Protection" of such Community data but addresses only the harnessing of the value of such data for community benefit if in anonymized form.* *Identifiable Joint/Community data therefore is not protected by both the regulations and there is a potential privacy issue if it is not protected by lawful processing.* *Hence there is need to define "Joint Personal Data" and "Joint Data Principal" and bring it within the ambit of the Personal data protection.* *Hence two additional definitions for "Joint Personal Data" and "Joint Data Principal" have been suggested.*	**of profiling, including the data about a Hindu Undivided Family.**
6	3(xy)	**Additional**		**(xy) Joint Data Principal/s means two or more living natural persons to whom the personal data relates**
7	3(xz)	**Additional**	*Anonymization is an important element of this regulation as it defines the boundary between Personal data and Non personal data.*	**3(xz) De-Anonymization** **De-anonymization means converting "anonymized personal data" which has been subjected to a standard irreversible**

			Until data is anonymized, it belongs to the regulation under this Act and post Anonymization, the data escapes the PDP regulation. *The Act presently defines de-identification but does not define De-anonymization* *To avoid confusion of these two terms, it is suggested that the definition of de-anonymization is added* *De-anonymization arises only if anonymization fails. But just as encryption or hashing is broken, anonymization may also be broken through a persistent criminal attack.* *In order to protect the integrity of the personal data protection it is necessary to criminalize de-anonymization. Otherwise like "Ethical hackers" turning into "Black hat hackers", technology persons will resort to de-anonymization as a routine practice.* *This requires a definition to be given for de-anonymization and punishment to be*	**anonymization process as per Section 3(2), to a state where it can be identified as personal data either partially or fully, whether accurately or not.**

			prescribed under section 82	
8	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	*The Committee on Non-Personal data governance has suggested that consent may be made necessary for anonymization.* *However Anonymization should be considered as the legitimate interest of an organization subject to the standards of anonymization to be set by the DPA.* *Hence "Anonymization" should be considered as one of the "Other purposes for which a specific permission is not required.* *At the same time, if "Anonymization" is not as per the irreversible standard set by the Authority, it would amount to negligence by the Data Fiduciary.* *If the anonymization meets the standard in ordinary circumstances but it still reversed by application of technology by some other person, it should be considered as a serious offence for which deterrent punishment is provided.*	**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—

		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; (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	*Necessary suggestions have been made in this set of recommendations accordingly.*	(a) prevention and detection of any unlawful activity including fraud; (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. **(i) Anonymization as per the standards to be prescribed by the authority.** (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.

		having regard to the fact whether such provision shall substantially prejudice the relevant reasonable purpose.		
9	16(2) and 16(3)	(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.	*A Data Fiduciary will come to know if a data subject is a minor or not only after the verification of age.* *Hence Section 16(2) would require age verification in all cases which is not practical.* *The need for age verification is therefore to be linked with the purpose for which a content is presented or consent for personal information is sought.* *Hence the suggestion is made*	(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) Whether the personal data is meant to be collected for a purpose of delivering a service that is expected to be used by a child** **(d)** possibility of harm to child arising out of processing of personal data; and **(e)** such other factors as may be prescribed.

10	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 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	*The data principals who may exercise their rights include both Citizens of India and non Citizens of India.* *The Constitutional mandate for the Government is to protect the Privacy of the Indian Citizens. However as per the definition of the "Data Principal" in Section 2, the rights guaranteed under this Act become available to foreign citizens also.* *When Indian data fiduciaries undertake processing of the personal data of foreign citizens as a part of their contract based processing activity, exemption can be claimed under Section 37.* *But when Indian data fiduciaries transact with foreign visitors, students and travellers, issues may arise on their rights.* *Of these, right to forget is already subject to adjudication.* *But right to access, right to correction and erasure as well as right to portability is applicable to such data principals and when invoked, cause*	**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 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

		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.	*significant disruption of the activities of small entities.* *The privilege of rights under Sections 18,19 and 20 requires to be regulated to avoid harassment of Indian Data Fiduciaries for alleged violations of privacy of foreign citizens each of whom would be interpreting the provisions with reference to their own culture and laws with which they are familiar with.* *To avoid frivolous complaints, a suggestion is made to route all such complaints through the DPA and also a mandatory mediation process before it is turned over to the Adjudication process.*	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. **(6) where the request for exercising any right is made by a data principal who is not a citizen of India,** **(a)not withstanding anything contained in Section 32 of the Act, the written reasoned request shall be made to the DPA who, after evaluating the nature of the alleged harm, may reject the request if the request is not reasonable.** **(b) If DPA finds the request to be reasonable, he shall notify the concerned Data Fiduciary and initiate a resolution process through mediation** **(c) If the complainant is not satisfied with the resolution, he may**

				submit his complaint to the adjudicator.
11	22(4)	(4) The privacy by design policy certified under sub-section (3) shall be published on the website of the data fiduciary and the Authority.	*The need to publish the privacy by design policy on the website of the DPA gives raise to some concerns that certain confidential information which may be considered as trade secrets of a data fiduciary may get exposed.* *Hence a suggestion is made that redaction of certain confidential aspects can be considered in the published version of the privacy by design policy.*	(4) The privacy by design policy certified under sub-section (3) shall be published on the website of the data fiduciary and the Authority, **Provided that the Authority may approve redaction of any parts of the policy that may be considered as confidential and disclosure of which may have an adverse impact on the data fiduciary.**
12	30(1)	(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	*The DPO needs support of the management to discharge his/her duties as envisaged under the Act.* *However since there could be a possibility that the DPO may have to deal with senior co workers and often bring out information which may be in conflict with some business interests, he/she is likely to be denied access to some information or otherwise prevented from working independently.* *Hence the suggestion is made to ensure that unreasonable pressure*	(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

		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; (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.	*is not brought on the DPO by the management leading to compromise of his responsibilities.*	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; (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. **(h) The Data Fiduciary shall provide necessary resources to the DPO to enable him discharge his responsibilities as envisaged** **(i) Appointment of a DPO and any changes thereof shall be reported to the Authority within a reasonable time.** **(j) The DPO shall not be personally liable for adverse consequences**

				while discharging the envisaged duties, unless a dishonest and fraudulent or otherwise malicious intention is involved.
13	30 (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.	*The Data Protection officer by virtue of section 30(2) appears to be only an employee of the Data Fiduciary. For SMEs it would be difficult to procure the services of qualified DPOs at a reasonable cost nor it may be necessary.* *Hence provision should be made for DPOs to be appointed as external consultants as in the case of Company secretaries and Chartered Accountants. Also this will enable better expertise to be available for complicated businesses.* *Also in the interest of independence of the office of DPO certain suggestions are made.*	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 **or from appointing an external entity as a DPO on a contractual basis Provided:** **1.where an external DPO has been appointed, a suitable employee of the organization shall be designated as a compliance official to assist the external DPO** **2. A Group of undertakings may appoint a single DPO provided the DPO is easily accessible to each of the group establishments.**
14	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	*Sections 33 and 34 refer to the Restrictions on transfer of personal data outside India. Compared to the first draft of PDPB-2018, the current bill has no restrictions for personal data being transferred out of India.* *The global trend however is to allow*	**Transfer of personal data outside India** **Subject to the conditions in section 34, personal data or Sensitive Personal Data may be transferred outside India, to such countries who have adequate data protection measures approved by the Authority in consultation**

		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.	*transfer of personal data only to such countries which can provide adequate protection to the personal data since it represents an obligation of the Government to protect the Privacy of the data subjects.* *Allowing free transfer of personal data as per Section 33 in the draft PDPB 2019 is therefore ultra vires the mandate for this law.* *The EU has recently tightened its restrictions on transfer of personal data and invalidated the US privacy shield since it was considered inadequate to protect the rights of the EU citizens.* *Hence "Adequacy" or "Appropriate contractual bindings" should be an essential requirement of transfer of personal data outside India.* *This has to be built into sections 33 and 34 which need an elaborate revision.* *Additionally it is considered an opportunity for India to lead a group of*	**with the Central Government.** **Provided that such approval shall be provided, only if it is satisfied that the country to which personal data is sought to be transferred provides** **(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) Adequate remedies are made available for Data Principals under this Act to exercise their rights in those countries, for any harm caused due to non-compliance of the provisions of the Act**
15	34	**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		**34. Conditions for transfer of personal data out of India** **(1) No restrictions shall apply for transfer of Personal Data to countries within the approved group of countries as indicated in Section 33, provided a concurrently updated copy of the data is kept in India.** **(2) Sensitive personal data may be transferred**

		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,	*countries which may agree to work on a common platform for mutual benefit respecting the laws of each other, protecting the democratic rights of the citizens of each of these countries.* *Further, under the proposed Non Personal Data Regulation there is an attempt to unlock the value out of Personal Data which is anonymized.* *This requires that Personal data should be considered as a potential asset and has to be preserved within India* *The modifications to Sections 33 and 34 are suggested in this context.*	**to countries within the approved group of countries for the purpose of processing, when explicit consent is is available from the data principal for such transfer, and where—** **the transfer is made pursuant to a legally binding contract or intra-group scheme approved by the Authority:** **(3) Notwithstanding anything contained in subsections (1) and (2) above, any personal data including sensitive or critical personal data may be transferred outside India, where such transfer is—** **To meet emergency health requirements of a data principal or any other person to an entity engaged in the provision of health services or emergency services where such transfer is necessary for prompt action under subsections (d), (e) and (f) of section 12;** **(4) Any transfer under subsection (3) above shall be notified to the Authority within such period as may be specified by regulations.**

		having regard to the applicable laws and international agreements; and (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.		
16	37	**Power of 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	*This section involves the processing of personal data of non Indians by the Indian data processors either in Indian territory or in a foreign territory.* *Such data processing comes within the provision of the Act solely because the activity occurs in India or the data fiduciary or processor is constituted in India.* *However, since the data does not belong to*	**Power of Central Government to exempt certain data processors.** The Authority may, on application exempt any Data Processor in India from the application of this Act, in respect of 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

		outside the territory of India, by any data processor or any class of data processors incorporated under Indian law.	*Indians, there is no constitutional obligation to include this in the Act and can be provided a general exemption for which a separate notification from the Government may not be required.* *However DPA may have a registration and approval system to ensure that such contractual data processing is monitored and regulated without adversely impacting the interest of the country.* *When Indian data processors enter into contracts with international data suppliers, there is a practice with the International Data Controllers to impose unreasonable and illegal contractual obligations on Indian data processors.* *The Standard Contractual clauses used by Data Exporters prohibit Indian law enforcement agencies to access the data processed even when it is considered necessary.* *Companies in India out of business compulsions sign indemnity*	incorporated outside the territory of India. **Provided further that the terms in such contracts shall not contravene any applicable Indian law and** **No liability under the contract shall be enforceable against the Indian entity except with the prior approval of the Authority.**

			contracts beyond their capacity. This could end up in Data Processors going insolvent affecting the Indian interests. *This needs to be placed under the supervision of the DPA*	
17	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 (c) the volume of	*The exemption provided under Section 39 is limited to manual processing only.* *In view of the operations of GST most of Indian small entities use computers to process their transactions which may involve personal information processing.* *Hence exemption may be provided even for automated processing.* *Regulations may prescribe different criteria to determine the applicability for manual and automated processing.*	**Exemption for 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.** (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 (c) the volume of personal data processed by such data fiduciary in any one day in the preceding twelve calendar months.

		personal data processed by such data fiduciary in any one day in the preceding twelve calendar months.		
18	49(4)	Additional	*There are instances where certain data fiduciaries such as registrars of domain names and E Mail service providers refuse to disclose certain data requested for lawful purpose under the excuse of privacy laws of their countries. As a result, a recipient of an e-mail does not get the originating IP address of the sender of the email. Similarly the registrant of a domain name who is suspected to have sent a phishing mail or communication hides his identity through the registrar even when the request is made by the recipient of the mail. These practices should be regulated. Presently the information may be requested only when a criminal case is filed and the request is made by a law enforcement authority.*	**(4) The Authority shall have the power to direct a data fiduciary providing a service of delivering an electronic communication to a data principal through any messaging service including an e-mail service or domain name related service, to provide information about the origin of the sender of the message when sought for by the receiver of the communication without demur, provided further that where the data fiduciary is not traceable or fails to respond, the Authority may direct the adjudicator to provide a suitable remedy.**
19	50(g)	processing of sensitive personal data under Chapter III;	*A Typographical error to be corrected*	processing **of personal data** under Chapter III;
20	62 (1)	For the purpose of adjudging the penalties under	*The section indicates as if the Adjudicating*	For the purpose of adjudging the penalties under sections 57 to 61or

		sections 57 to 61or awarding compensation under section 64, the Authority shall appoint such Adjudicating Officer as may be prescribed.	*officer is an employee of DPA.* *Since Adjudication is a specialized activity, it is not possible to provide a full career for the Adjudicators as employees.* *Hence it is preferable to appoint adjudicators on a contract basis.*	awarding compensation under section 64, the Authority shall appoint such Adjudicating Officer as may be prescribed **under a contract for a period not exceeding 5 years.**
21	67(2)	(2) The Appellate Tribunal shall consist of a Chairperson and not more than members to be appointed.	*Number of members omitted*	The Appellate Tribunal shall consist of a Chairperson and **not more than Three members** to be appointed.
22	82(1(a)	(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	*This section has two issues. One is that "De-identification" is often used by the Processor during the processing operation to be re-identified at the end of the processing chain to reduce the risk of wrong disclosure within the organization.* *This is different from a party other than the Data Fiduciary or Data Processor doing a de-identification.* *Hence "De-Identification by another data fiduciary" alone should be punishable and not by the same data fiduciary.*	**(1)(a) Any person who, with dishonest fraudulent or malicious intention— re-identifies and/or processes personal data which has been de-identified by another person, without his consent,** **shall be punishable with imprisonment for a term not exceeding three years or with a fine which may extend to two lakh rupees or both on the first instance and with a term of 5 years and a fine upto Rs 5 lakhs for subsequent offence/s.** **(b) Any person who, with dishonest, fraudulent or malicious intention—**

			Secondly there is a natural confusion in the words de-identification and anonymization and correspondingly the terms of "Re-identification" and "De-Anonymization". *This needs to be clarified.* *It is also suggested that an enhanced punishment for de-anonymisation may be prescribed.* *Further in both cases of de-identification and de-anonymisation, higher punishment for repeated conduct is suggested*	**De-anonymizes an anonymized personal data by any means** **shall be punishable with imprisonment for a term not exceeding Five years or with a fine which may extend to Five lakh rupees or both on the first instance and with a term of 7 years and a fine upto Rs 10 lakhs for subsequent offence.**