# DUCTUS LEGAL FIRM

DUCTUS LEGAL
CORPORATE LAWYERS & LEGAL CONSULTANTS

# PERSONAL DATA PROTECTION BILL, 2019

## INDIA'S APPROACH TOWARDS DATA PROTECTION

**Author: Gargi Singh, Associate, Ductus Legal**
**www.ductuslegal.com, dixit@ductuslegal.com**

**Ductus Legal, 109, First Floor, Modi Tower, Nehru Place, South Delhi-19**

# PERSONAL DATA PROTECTION BILL, 2019

Right to Privacy is a fundamental right as per Article 21 of the constitution of India. The constitutional bench in "***K.S. Puttaswamy Anr. vs. Union of India" while giving their final verdict had emphasized upon right to privacy in the year 2018 and stressed upon 'robust data protection regime'***. The Government on 31st July, 2017 had constituted a "Committee of Experts on Data Protection" chaired by Justice B.N. Srikrishna for examining the issues pertaining to data protection. The Committee had examined the issues on data protection and submitted its Report on 27th July, 2018. On the basis of the recommendations made in the said Report and the suggestions received from various stakeholders, it was proposed that a legislation should be enacted, namely, the Personal Data Protection Bill, 2019. **The Personal Data Protection Bill was introduced in the Lok Sabha by the Minister of Electronics and Information Technology on December 11th December 2019.** It can be understood from the introduction that protection of personal data is our right to privacy.

Before dwelling further into the bill, **it is pertinent to note the definition of *Personal Data* as defined under *section 3(28)*.The personal data is defined as "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 bill seeks to provide protection to the personal data of natural persons (data principles) having their personal data online or offline. After reading the bill, it can be inferred that the bill has categorized Personal data into sensitive personal data and critical personal data. The ingredients to constitute Sensitive personal Data and Critical Personal Data are exhaustive and Central Government in official gazette shall notify the constituents of Critical Personal Data. What constitutes as the Sensitive Personal Data has been defined in **section 3(36) and shall include financial data; health data; official identifier; sex life; sexual orientation; biometric**

[1] Definition of Personal Data under Section 3(28) of the Personal Data Protection Bill 2019.

**data; genetic data; transgender status; intersex status; caste or tribe; religious or political belief or affiliation; or any other data categorized as sensitive personal data under section 15**[2]. Section 15 lays down the categorization for a personal data when it will constitute as sensitive personal data. If the data would constitute significant harm to the natural person, or there is a level of confidentiality attached to such data, a significantly discernible class of data principals may suffer significant harm if such category of data is processed and adequate protection is provided by ordinary provisions applicable to such personal data, then in all these circumstances it will be presumed that the personal data is a sensitive personal data. Explanation to section 33 states that constituents of Critical personal data shall be notified by the Central Government. Chapter VII talks about Restriction on Transfer of Personal Data outside India and Section 33(1) states that 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 [3]whereas Section 33(2) states that the critical personal data shall only be processed in India.[4]

Before talking about the conditions, it is pertinent to note the definition of intra-group scheme

*Section 3(22)* defines *intra-group scheme* as " the schemes approved by the Authority under clause (a) of sub-section (1) of section 34;"[5] The conditions specified in Section 34(1)(a)(i) and (ii) are that the explicit consent of data principal shall be required and if the transfer is made pursuant to a contract or intra-group scheme approved by the Authority but such scheme shall not be approved unless the scheme has provisions for effective protection of the rights of the data principal under this Act, including in relation to further transfer to any other person; and 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;[6]

From the language of section 31, it can be understood that the sensitive personal data and critical 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 the Central Government, after consultation with the Authority, has allowed the transfer to a country or, to such entity or to class of entity in a country or, to an international organization on the basis of its finding that such

[2] Definition of Sensitive Personal Data under Section 3(36) of Personal Data Protection Bill 2019.
[3] Section 33(1) of Personal Data Protection Bill 2019.
[4] Section 33(2) of Personal Data Protection Bill 2019.
[5] Section 3(22) of Personal Data Protection Bill 2019.
[6] Section 34(1)(a)(i) and (ii) of Personal Data Protection Bill 2019.

sensitive personal data and critical persona data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements; such transfer shall not prejudicially affect the enforcement of relevant laws by authorities with appropriate jurisdiction ,the Authority has allowed transfer of any sensitive personal data or class of sensitive personal data necessary for any specific purpose., any critical personal data may be transferred outside India, only where such transfer is 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 to a country or, any entity or class of entity in a country or, to an international organization, where it will be provided with adequate level of protection and would not prejudicially affect the enforcement of relevant laws by authorities with appropriate jurisdiction: where the Central Government has deemed such transfer to be permissible and where such transfer in the opinion of the Central Government does not prejudicially affect the security and strategic interest of the State. Any transfer under 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 12shall be notified to the Authority within such period as may be specified by regulations.[7]

Before discussing about the applicability of the act, I will provide the definition of data fiduciary, data processor, processing, profiling, anonymised and anonymisation.

*Section 3(13)* defines *data fiduciary* as "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;"[8]

*Section 3(15)* defines *data processor* as "any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary;"[9]

*Section 3 (31)* defines *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,

[7] Section 34 on Conditions for transfer of sensitive personal data and critical personal data.
[8] Definition of Data Fiduciary in Section 3(13) of Personal Data Protection Bill 2019.
[9] Definition of Data Processor in Section 3(15) of Personal Data Protection Bill 2019.

indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;"[10]

*Section 3 (32)* defines *profiling* as "any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a data principal;"[11]

*Section 3(3)* defines *anonymised data* as "data which has undergone the process of anonymisation;"[12]

*Section 3(2)* defines *anonymisation* as "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;"

As per the language of section 2(A)(c)(i) and Section 2(A)(c)(ii), the bill will have extra-territorial application. It means that data fiduciaries or data processors that do not reside in India but if data fiduciaries or data processors are carrying out any business in India, providing any goods or services to data principles(natural persons) residing in India or profiling the data of residents of India then this bill shall be applicable on such data fiduciaries or data processors. The bill shall only apply to anonymised data referred in Section 91. Section 91 states that "Central Government after consultation with Data Protection 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."[13] the expression *non-personal data* means the data other than personal data.[14] It is not clear as to what shall constitute a non-personal data but it is understood that the applicability of the act is on the personal data as well as non-personal data and data fiduciary and data processors can be asked to disclose and provide anonymised personal data and non-personal data to the Central Government. The question that could arise is on what anonymised data shall the act would not apply on? The government should clarify this question in the bill before it becomes an act.

[10] Definition of Processing in Section 3(31) of Personal Data Protection Bill 2019.
[11] Definition of Processing in Section 3(32) of Personal Data Protection Bill 2019.
[12] Definition of Anonymized Data in Section 3(3) of Personal Data Protection Bill 2019.
[13] Section 91(2) of Personal Data Protection Bill 2019.
[14] Explanation to Section 91(2) of Personal Data Protection Bill 2019.

Chapter II of the bill states the obligations of data fiduciaries. Section 7 of the bill states that the data fiduciary shall provide a notice to data principles informing them regarding the purpose of processing, rights available to data principles for withdrawing their consent and procedure for such withdrawl if personal data was intended to be processed on the basis of consent. If personal data is supposed to be processed on the basis of section 12 to section 14 i.e., grounds for processing without consent then consequences for not providing the personal data. Data fiduciaries are obligated to inform data principles if the personal data would be shared with other individuals or entities, source of collection of such personal data if such data wasn't collected from data principal himself/herself, information regarding cross border transfer of personal data if such transfer is being intended to carry out, the procedure for grievance redressal under section 32, the existence of a right to file complaints to the Authority etc. Section 32 states that every data fiduciary is obligated to have a grievance redressal mechanism for data principle if data principal wants to file a complaint. In case of significant data fiduciary, then complaint can be filed to data protection officer and in case of other data fiduicaries then the complaint can be filed to officer designated. The complaint should be resolved within thirty days. If data principal is not satisfied with the manner in which the complaint was resolved then complaint can be filed to authority in a prescribed manner.[15]

Section 10 fixes the responsibility and accountability of data fiduciary for complying with the provisions of the act even in cases where data is processed on its behalf by data processor. Data fiduciary shall be severally liable as per section 10.Section 11 talks about mandatory consent taken from data principle in cases where the consent is necessary for processing. Consent of data principal should be free, informed under section 7,specific for the scope in respect for purpose of processing, clear by an affirmation action that is meaningful, capable of being withdrawn having regard to the ease with which it can be withdrawn in comparison with the ease the consent was given. If processing of sensitive personal data is to be taken then data fiduciary in clear terms has to inform data principal about purpose of processing and operation in processing which is likely to cause significant harm to the data principal. Further providing the data principal with the choice of separately consenting to the purpose, operation in processing and use of different categories of sensitive personal data.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

[15] Section 32 Grievance Redressal by Data Fiduciary

not be made conditional on the consent to the processing of any personal data not necessary for that purpose.[16]The burden of proof shall be on data fiduciary.

Section 12 talks about grounds for processing of personal data without consent. The language of section 12 begins with 'notwithstanding anything contained in Section 11' which means that even sensitive personal information can be processed without consent for performance of any function of State authorized by law for the purpose of any service or benefit or for issuance of any license, certification or permit by the State, under any law made by parliament or State Legislature, for compliance with any order and judgment of the court or tribunal in India or in cases of threat to public life, public health or disaster or any breakdown of public order. As per section 14 personal data can be processed for 'reasonable purposes' such as prevention and detection of any unlawful activity including fraud; whistle blowing;mergers and acquisitions; network and information security; credit scoring; recovery of debt; processing of publicly available personal data; and the operation of search engines. [17] Another important provision take note of is that if notice under section 7 is prejudical to the purpose of processing then notice informing data principal regarding the processing of his/her personal data would not be provided to data principal for the purpose of this section.

Section 16 talks about processing of personal data and sensitive personal data of children. The authority shall classify a data fiduciary as guardian data fiduciary who operates commercial website or online services directed at children and processes large volume of personal data of children. 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.[18]Further guardian data fiduciary is barred from profiling, tracking or behaviouraly monitoring of or targeted advertising directed at children and undertaking any other processing of personal data that can cause significant harm to the child[19]. The provision shall also apply of in such modified form to the data fiduciary offering counselling or child protection services to a child, as the Authority may by regulations specify.[20] A guardian data fiduciary providing

[16] Section 11 (4) of Personal Data Protection Bill 2019.
[17] Section 14(2) of Personal Data Protection Bill 2019.
[18] Section 16(2) of Personal Data Protection Bill 2019.
[19] Section 16(5) of Personal Data Protection Bill 2019.
[20] Section 16(6) of Personal Data Protection Bill 2019.

exclusive counselling or child protection services to a child shall not require to obtain the consent of parent or guardian of the child.[21]

Chapter V talks about rights of data principals. Data Principal has 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 that has been shared with such data fiduciaries, in such manner as may be specified by regulations.[22] As per section 18, the data principal has the right to correction of data which has an inaccurate or misleading information and erasure of such personal data which is not required further for the purpose of processing. Where the data fiduciary corrects, completes, updates or erases any personal data 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.[23] Under Section 19,the Data Principal has the right to data portability wherein the data principal shall have the data in a 'structured and machine readable format'[24] The Data Principal shall not have the right to data portability in case wherein section 12 is applicable as per which the personal data including sensitive personal data is processed without consent to exercise functions of the state or authorized under any law. Further data principal's right to data portability cannot be exercised if it would 'reveal a trade secret' or is not 'technically feasible'.[25] Section 20 talks about the data principal's right to be forgotten if continued disclosure of his personal data has served the purpose, the consent provided under section 11 has been withdrawn by data principal or the personal data was collected contrary to the provisions of the bill or any law in India.[26] To enforce the right,the data principal would need to apply to the adjudicating officer who would pass an order provided that such continued disclosure of personal data is overriding the right to freedom of speech and expression of data principal and right to information of any other citizen.[27] On further reading of the provision, it can be ascertained that consideration shall also be given to

[21] Section 16(7) of Personal Data Protection Bill 2019.
[22] Section 17(3) of Personal Data Protection Bill 2019.
[23] Section 18(4) of Personal Data Protection Bill 2019.
[24] Section 19(1)(a) of Personal Data Protection Bill 2019.
[25] Section19(2)(b) of Personal Data Protection Bill 2019.
[26] Section 20(1) of Personal Data Protection Bill 2019.
[27] Section 20(2) of Personal Data Protection Bill 2019.

data fiduciary if 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.'[28]

As per Section 21, Data Principal for exercising the right to confirmation and access under section 17,right to correction and erasure under section 18,right to data portability under section 19 can directly or indirectly make a request to data fiduciary or through a consent manager. 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."[29] The consent manager is required to be registered with the authority.[30]

Chapter VI lays down Transparency and Accountability Measures. Section 22 states that data fiduciary has to submit 'privacy by design policy' to the authority for its approval mentioning about organizational structure as well as obligations. If the authority is satisfied with the compliance then shall issue a certificate. While reading the language of section 24 the 'methods such as de-identification and encryption' would depend on likelihood of harm associated with processing and such likelihood of harm is present in case of processing of sensitive personal data. Section 26 classifies data fiduciaries as significant data fiduciaries depending upon the factors such as volume of personal data processed; sensitivity of personal data processed;turnover of the data fiduciary; risk of harm by processing by the data fiduciary; use of new technologies for processing; and any other factor causing harm from such processing.[31] Any social media intermediary with users above such threshold as may be notified by the Central Government, in consultation with the Authority; and 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 India, shall be notified by the Central Government, in consultation with the Authority, as a significant data fiduciary:[32] Explanation to section 26(4) creates an ambiguity for the purpose of defining social media intermediary because the reading of the section begins as 'For the purposes of this sub-section', which means that otherwise while defining social media intermediary, this definition provided in the explanation may not be considered. A social media

[28] Section 20(3)(e) of Personal Data Protection Bill 2019.
[29] Explanation to Section 23 defines Consent Manager.
[30] Section 23(5) of Personal Data Protection Bill 2019.
[31] Section 26 (1) (a) to (f) of Personal Data Protection Bill 2019.
[32] Section 26(4) of Personal Data Protection Bill 2019.

intermediary is defined as "who 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, but shall not include intermediaries which primarily, enable commercial or business oriented transactions; provide access to the Internet; in the nature of search-engines, on-line encyclopedias, e-mail services or online storage services"[33] Whereas *Section 2(w)* of IT Act as amended till now defines *intemediary* "with respect to any particular records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes."[34] Under explanation to section 26(4) the definition of social media intermediary is quite similar to that of intermediary under IT act except definition of social media intermediary excludes internet service providers or intermediaries that enable commercial or business oriented transactions. It may mean that these excluded categories from definition of social media intermediary will be just referred to as data fiduciaries for the purpose of this bill. It can be inferred from the language of section 26(3) that if 'processing carries a risk of significant harm to data principals' then section 27,section 28,section 29 and section 30 would be made applicable on such data fiduciaries by authority but these sections are impliedly applicable on 'significant data fiduciaries.'[35] Another relevant provision in this chapter in section 27 which states that every significant data fiduciary like social media intermediary would have to carry out Data Protection Impact Assessment in case of processing of sensitive personal data prior to processing. Such Data Protection Impact Assessment is not limited to significant data fiduciaries but also in cases where data fiduciaries not being significant data fiduciaries may be asked to conduct such assessment prior to processing if processing may cause significant harm to a data principal.[36]For the purpose of section 27 the authority shall specify instances where data auditor shall be appointed by data fiduciary to carryout assessment after completion of Data Protection Impact Assessment the report shall be submitted to data protection officer who is also appointed by data fiduciary such data protection officer would review the assessment and submit the report to the authority.

[33] Explanation to Section 26(4) of Personal Data Protection Bill 2019.
[34] Section 2(w) of IT Act.
[35] Section 26(3) of Personal Data Protection Bill 2019.
[36] Id.

Authority would then decide whether to begin with processing with conditions or cease the processing if it will likely cause significant harm to data principals.[37]As per section 29 the significant data fiduciary or data fiduciaries not being significant data fiduciaries have to appoint an independent data auditor annually to review their policies. The data auditor has to be registered with the authority and may provide data trust score to data fiduciaries. Section 31 states that 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. The data processor shall not engage, appoint, use, or involve another data processor in the processing on its behalf, except with the authorization of the data fiduciary and unless permitted in the contract.[38]Section 32 talks about Grievance redressal by data fiduciary. In case the processing is likely to cause harm to data principal then complaint shall be filed with 'the data protection officer, in case of a significant data fiduciary; or an officer designated for this purpose, in case of any other data fiduciary.'[39]

Chapter VIII provides exemptions such as under section 35, the power of Central Government to exempt any agency of government from the application of the act. Power of exemption of certain provisions for certain processing of personal data except section 4 and section 24 that would still apply. Section 4 talks about lawful processing and section 24 which talks about when processing is likely to cause significant harm. Further certain provisions of the act shall not apply on small entity. a "small entity" means such data fiduciary as may be classified, by regulations, by Authority, having regard to the turnover of data fiduciary in the preceding financial year; the purpose of collection of personal data for disclosure to any other individuals or entities; and the volume of personal data processed by such data fiduciary in any one day in the preceding twelve calendar months.[40] One of the provisions that is not applicable on small entity is section 20.Section 20 talks about the Data Principal's right to restrict or prevent the continuing disclosure of his personal data by a data fiduciary and clause (b) of Section 20 states that "if the disclosure was made with the consent of the data principal under section 11 and such consent has since been withdrawn". Now the ambiguity is that Section 11 is not explicitly stated as non-applicable on small entity processing data through manual means therefore section 11 will be

[37] Section 27 of Personal Data Protection Bill 2019.
[38] Section 31(1) and (2) of Personal Data Protection Bill 2019.
[39] Section 32(2)(a) and (b) of Personal Data Protection Bill 2019.
[40] Section 39(2) defines small entity of Personal Data Protection Bill 2019.

applicable which means that small entity is mandatorily required to take the consent from data principal and data principal can also withdraw his/her consent. Section 20 is contradictory with section 11.Thereore it should be clarified as to who could be declared as small entity. Probably the regulations shall clarify the discrepancies in the definition of small entity as well as reasons for non-applicability of certain relevant provisions such as transparency and accountability measures on small entity. Section 40 talks about 'Sandbox'. Section 40(1) states "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."[41] The term of the inclusion in the Sandbox, cannot be renewed more than twice, subject to a total period of thirty-six months.[42]Any data fiduciary can apply for inclusion in the sandbox but 'small entity' cannot apply for the same since section 22 is not applicable on small entity which talks about privacy by design policy which is required to be mandatorily prepared by data fiduciary to be included in the sandbox. A data fiduciary is required to inform about the data principals participating in the proposed processing for the purpose of sandbox.[43] Other relevant information to be furnished by such data fiduciary includes "the requirement of consent of data principals participating under any licensed activity, compensation to such data principals and penalties in relation to such safeguards."[44] Ambiguity arises in Section 40(4)(c) wherein certain provisions of the bill 'shall or shall not apply in modified form' on such data fiduciary. Such provisions are Section 40(4)(c)(i), Section 40(4)(c)(ii) and Section 40(4)(c)(iii).

Section 40(4)(c)(i) states that obligation to specify clear and specific purpose 'shall or shall not apply in modified form' but the purpose is clear that is why a data fiduciary would want to be included in the sandbox. Further section 4 also includes the word 'lawful'. Section 40(4)(c)(ii) talks about 'limitation on collection of personal data under section 6' wherein section 6 states that "data shall be collected only to the extent that is necessary for the purposes of processing of such personal data."[45] Sandbox would be formed with clear purpose i.e., for promoting Artificial intelligence therefore isin't it implied that data should be collected to the extent that is necessary for the purpose, so why section 6 'shall or shall not' apply in modified form. Such section should apply on sandbox and confusion related to 'shall or shall not' apply in modified form should

[41] Section 40(1) of Personal Data Protection Bill 2019.
[42] Section 40(4)(a) of Personal Data Protection Bill 2019.
[43] Section 40(3)(c) of Personal Data Protection Bill 2019.
[44] Section 40(4)(b) of Personal Data Protection Bill 2019.
[45] Section 6 of Personal Data Protection Bill 2019.

either be cleared or removed. Section 40 clearly states that data principles would be participating in the sandbox after data fiduciary has taken their consent. Section 5 talks about 'Limitation on purpose of processing of personal data.' Further Section 5(b) states that "Every person processing personal data of a data principal shall process such personal data for the purpose consented to by the data principal or which is incidental to or connected with such purpose,".[46]Further Section 40(4)(c)(iii) states that "following obligations shall not apply or apply with modified form to such data fiduciary, namely any other obligation to the extent, it is directly depending on the obligations under sections 5 and 6;".Such data fiduciary planning to be included in a sandbox is mandatorily required to take consent from data principals in section 40 and even the language of section 5 talks about mandatorily processing for the purpose for which the consent was taken. Therefore what cannot be understood is in what modified form the provisions shall or shall not apply on sandbox.

Section 49(3) states that when Data Protection Authority shall process personal data then it shall be construed as data fiduciary or data processor. Probably the regulations will specify the circumstances when the Authority shall become a data fiduciary or data processor. The next part of the provision states that "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 under any law to do so, or where it is required to carry out its function under this section."[47]What if disclosing the information is in public interest then will the information be disclosed? Section 50 talks about the 'code of practice' for promoting good practices of data protection.[48]The Authority may approve the code of practice submitted by industry or trade association, an association representing the interest of data principals, any sectoral regulator or statutory Authority, or any departments or ministries of the Central or State Government.[49]Code of practice shall specify the manner of processing of personal data or sensitive personal data as well as procedure for obtaining consent under section 11, technical and safety measures adopted by data fiduciaries while processing data etc. Language of Section 53 and Section 54 states that proper procedure shall be adopted which includes appointment of one of the officers as inquiry officer who shall perform the functions of a civil court under civil

[46] Section 5(b) of Personal Data Protection Bill 2019.
[47] Section 49(3) of Personal Data Protection Bill 2019.
[48]Section 50(1) of Personal Data Protection Bill 2019.
[49] Section 50(2) of Personal Data Protection Bill 2019.

procedure code and conduct inquiry subsequently submit a report to the authority on the basis of which the authority shall by an order restrict the cross-border flow of personal data or pass any other order laid down in section 54(1). Section 56 states that if Authority under this act and any sector regulator may have a concurrent jurisdiction then both Authority and that sector regulator would consult each other and may enter into a memorandum of understanding.

Chapter X talks about Penalties and Compensation. It says that 'data fiduciary' shall be held liable but does not include 'data processor'. Penalty shall be imposed upon data fiduciary for contravening the provisions of the act, failure to comply with data principal requests under Chapter V that talks about rights of data principal, failure to furnish report, returns, information, failure to comply with direction or order issued by Authority and for contravention where no separate penalty has been provided.[50]Adjudication officer shall be appointed by the authority for adjudging penalties and awarding compensation. Section 62(3) talks about the qualification of adjudicating officer. Section 63(4)(c) talks about "intentional or negligent character of the violation" while adjudging penalty but the definition of 'personal data breach' under section 3(39) includes 'accidental disclosure' as a means of breach.[51]Section 64 talks about compensation. The language of section 64 clearly states that compensation shall be awarded to "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,"[52] For the purpose of right to seek compensation of data principal both data fiduciary and data processor are included against whom such compensation shall be awarded. Penalty shall be adjudged on the basis of complaint made by authority[53] while compensation shall be awarded by making a complaint to the adjudicating officer.[54]If a data principal is aggrieved by the order of adjudicating officer then an appeal can be filed with appellate tribunal.[55]Section 66(1) states that "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."[56]

As persection72 any appeal from data protection authority shall lie with Appellate Tribunal. Section 75 states that appeal from Appellate Tribunal shall be made to Supreme Court.

[50] Section 57 to Section 61 of Personal Data Protection Bill 2019.
[51] Section 3(39) of Personal Data Protection Bill 2019.
[52] Section 64(1) of Personal Data Protection Bill 2019.
[53] Section 63(1) of Personal Data Protection Bill 2019.
[54] Section 64(2) of Personal Data Protection Bill 2019.
[55] Section 64(7) of Personal Data Protection Bill 2019.
[56] Section 66(1) of Personal Data Protection Bill 2019.

It is pertinent to note the definition of re-identification and de-identification for this Chapter.

*Section 3(16*) defines *de-identification* as "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;"[57]

*Section 3(34)* defines *re-identification* as the "means the process by which a data fiduciary or data processor may reverse a process of de-identification;"[58]

Chapter XIII talks about offences. If a person re-identifies the de-identification procedure conducted on personal data by data fiduciary or data procedure "without the consent of such data fiduciary or data processor, then, such person shall be punishable with imprisonment for a term not exceeding three years or with a fine which may extend to two lakh rupees."[59]Section 82(2) lays down the exceptions wherein the 'person's' act shall not constitute an offence. The ambiguity pertains to section 82(2)(b) which states that if data principal whose data is in question has consented to re-identification then in such a case a person shall not be liable. On whom this provision is applicable whether on all data fiduciaries or only on government's agency because 'consent' can be taken through ambiguous contractual provisions which every data principal is not capable to comprehend the consequences of. Section 83(1) clearly states that "Notwithstanding anything contained in the Code of Criminal Procedure, 1973, an offence punishable under this Act shall be cognizable and non-bailable".[60] This chapter includes the offence by State and offence by companies as well.

Chapter XIV talks about other miscellaneous provisions. Section 88 states that "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."[61] What would happen in situations wherein Data Protection Authority itself is a data fiduciary or a data processor.[62]

---

[57] Section 3(16) of Personal Data Protection Bill 2019.
[58] Section 3(34) of Personal Data Protection Bill 2019.
[59] Section 82(1)(b) of Personal Data Protection Bill 2019.
[60] Section 83(1) of Personal Data Protection Bill 2019.
[61] Section 88 of Personal Data Protection Bill 2019.
[62] Section 49(3) of Personal Data Protection Bill 2019.

## CONCLUSION

Personal Data Protection bill has been adopted from General Data Protection Regulations. The bill seeks to protect personal data available online or offline. Data Protection Authority is authorized under the act to protect the personal data of natural persons. Data Protection Authority should be an independent authority and not under the control and influence of the Central Government to exercise its functions without unnecessary hassle. GDPR defines cross-border transfer whereas personal data protection bill does not define 'cross-border transfer' of personal data despite the fact that most of the significant companies operating in India have their data processors outside India for processing the personal data. Since data processors are outside it is pertinent in the interest of data principals to be aware of their data sharing activities. GDPR emphasizes upon protection of personal data as well as free flow of data while Personal Data Protection bill allows free flow of personal data to only an extent wherein sensitive personal data can be processed outside but has to be stored in India wherein critical personal data is to be processed only in India.