Comments on the Draft Digital Personal Data Protection Bill, 2022 |

Submission to the Ministry of Electronics and Information Technology

December 2022

V | D H | Centre for Legal Policy

About Vidhi

Vidhi Centre for Legal Policy ("Vidhi") is a not-for-profit independent think-tank doing legal research to make better laws and improve governance for the public good.

This is an independent, non-commissioned piece of work by Vidhi.

For any clarifications/ queries in relation to this submission, please email Ameen Jauhar, Senior Resident Fellow and Lead, Centre for Applied Law and Technology Research (ALTR), at ameen.jauhar@vidhilegalpolicy.in and Sunetra Ravindran, Senior Resident Fellow and Lead, Legal Design and Regulation, at sunetra.ravindran@vidhilegalpolicy.in

Summary of Comments

S. No.	Clause	Recommendation
1.	2(6)- Definition of Data Principal	The definition of Data Principal should not include the parents/legal guardians of a child (who is a data principal).
2.	2(10)- Definition of Harm	The definition of harm should be broadened to account for intangible forms of harm such as loss of reputation, loss of employment, discriminatory treatment, restrictions placed on speech or movement due to fear of being surveilled etc.
3.	2(18)- Definition of Public Interest	The definition of "public interest" should be deleted.
4.	4- Application of the Act	The law should be made applicable to all digital personal data or processing through automated means (whether online or offline).
5.	5- Grounds for processing digital personal data	This ground should also incorporate purpose limitation and collection limitation principles.
6.	6- Notice	The concept of notice must be made mandatory even where there are non-consensual grounds of processing. Any exceptions from the obligation of notice must be limited by conditions of necessity or where the legitimate purpose of processing is made impossible to carry out by the provision of notice. The information provided at the time of notice must also be expanded. Proactive disclosure of a privacy policy and the ordinary terms of data processing must also be provided for under the law.
7.	7- Consent	In relation to Clause 7(2)- consent which infringes the provisions of the Act- this concern may be addressed by creating a separate provision disallowing the waiver of data principal rights. This may be done for caution even though such waiver may be illegal under the doctrine of waiver. In relation to Clause 7(4)- withdrawal of consent- the provision for "consequences" of withdrawal of consent should be restricted to consent for processing personal data necessary for the performance of a contract.

		In relation to Clause 7(8)- making the enjoyment of rights conditional on grant of consent not necessary for the provision of those rights should be explicitly prohibited.
8.	8- Deemed Consent	This clause should be deleted as it dilutes informational autonomy. Consent should ordinarily be a ground for processing personal data only if some affirmative action is made to provide for this. Alternatively, the provision should be redrafted to contain further strict conditions such as: (a) Consent for processing personal data must be for a fixed purpose, even if such consent is implied; (b) Implied consent should be withdrawable; (c) It should be impermissible to use implied consent to process sensitive personal data or process any personal data in a way that may cause a risk of significant harm; and (d) further guidance may be provided on when consent may be implied for contractual necessity or on the provision of some form of notification.
9.	8(2)- 8(8) Non consensual processing	Sub-clauses (2) to (8) of clause 8 should be separated from sub-clause (1) and placed in a separate provision that is distinct from the concept of deemed consent and referred to as non-consensual grounds of processing.
10.	8(2)- Performance of functions of the State	The requirement of authorisation of law must be placed on any processing for provision of services or benefits and on processing for issuance of permits. Further, processing under this provision should only be for functions of the State or should at least exclude business activities
11.	(Omitted) Compliance with law	The appropriate placement for a ground for processing in compliance with a law is within the list of non-consensual grounds. It should be reintroduced there.
12.	8(7)- Employment Purposes	This provision should be restricted to listed employment purposes instead of being made open ended. Purposes related to confidentiality and intellectual property rights must be excluded entirely from this closed list. Safeguards must be introduced to ensure that this ground may only be

		employed where obtaining the consent of an employee is appropriate and feasible.
13.	8(8) and 8(9)- Public interest and fair and reasonable purposes.	The purposes listed in this sub-clause should not be referred to as "public interest" due to inconsistency with the definition of that term. The provisions which act as non-consensual grounds of data processing should be restricted by adequate safeguards that prevent disproportionate invasions into the rights of individuals or the risk of significant harm. The moniker of "fair and reasonable purpose" or "legitimate interest" would provide better guidance and precedent rather than "public interest". Sub-clauses (8) and (9) should not be available to State entities without authorisation of a law on the specific grounds and this may be stated explicitly within this clause.
14.	9- General obligations of data fiduciaries	The obligation of reasonable security safeguards should be extended beyond prevention of data breaches and should cover safeguards related to de-identification, encryption and data integrity. The obligation on storage limitation must limit the exception from purpose limitation to only those legal and business purposes that are legitimate or otherwise covered under grounds of processing, and any such exception should be made justifiable with provision of notice where applicable. Transfer of data from one data fiduciary to another should be permissible so long as it is necessary under one of the grounds of processing under Clauses 7 and 8.
15.	10- Additional obligations in relation to processing of personal data of children	The upper age limit of "child" should be reduced below 18. The definition of data principals should not extend to the parents and guardians of a child.
16.	12(2)- Right to information about personal data	The summary of data must be shared in a clear, concise and comprehensible manner.

17.	13(1)- Right to correction and erasure of personal data	The phrase 'in accordance with applicable laws is unclear and overbroad.
18.	13(2)(d)- Right to correction and erasure of personal data	The data principal's right to ask for erasure of any data which doesn't need to be retained for a legal purpose must be harmonised with Clause 9(6) where fiduciaries can retain data for business and legal purposes.
19.	13- Right to correction and erasure of personal data	Provision must include conflict resolution mechanism for disagreement between data principal and data fiduciary regarding correction or erasure.
20.	13- Right to correction and erasure of personal data	Data fiduciary must pass on the corrected information or erasure status to third parties with whom data has been shared.
21.	14- Right of grievance redressal	Human interface must be mandated for grievance redressal mechanisms to avoid reliance on automated processes.
22.	15- Right to nominate	'Unsoundness of body' must be reconsidered or clarified.
23.	16(1)- Duties of Data Principal	This provision can be omitted as it serves no additional functions and can be misused.
24.	16(2)- Duties of Data Principal	This provision can be omitted due to the potential for misuse and the resultant chilling effects, as well as the subjective interpretation of false or frivolous complaints.
25.	16(3)- Duties of Data Principal	The word 'including' must be omitted, and the requirement to furnish true information and to not suppress material facts to be limited to obtaining documents, services, unique identifiers, proof of identity or address from state institutions.
26.	17- Transfer of personal data outside India	Should provide criteria for notifying jurisdictions, taking into account equivalent data protection laws in that country and impact on enforcement of laws.
27.	18(1)(c)- Exemptions	Exemption must be qualified and limited to state agencies to prevent misuse.
28.	18(1)(d)- Exemptions	Exemption must be deleted due to lack of clarity on its purpose. Either it must be shifted to clause 4, or it raises concerns on adequacy.
29.	18(2)(a)- Exemptions	Exemption must be limited on grounds of necessity and proportionality. Timelines for exemption,

		alternative safeguards and oversight mechanisms must be framed for such exempted entities.
30.	18(2)(b)- Exemptions	Certain provisions must not be exempted. Further, only those exemptions must be granted if compliance with such provisions renders impossible or seriously impairs the purposes, and if data principal shall not be at risk of harm due to such processing.
31.	18(3)- Exemptions	Shift exemption from obligations under clause 18 to Clause 10. Exemption to Clause 11 can be omitted as it is redundant.
32.	18(4)- Exemptions	This provision can be omitted as it may fail the test of reasonable classification under Article 14 as well as the right to privacy.
33.	18- Exemptions	Exemptions for personal data processing for journalistic purposes and for literary, academic or artistic expression may be added to balance the right to free speech and expression under the Indian constitution.
34.	19(1)- Data Protection Board of India	Public-facing functions of the DPB must have alternatives to the 'digital by design' model to avoid exclusion.
35.	19- Data Protection Board of India	Safeguards must be added to ensure institutional and functional independence of the DPB.
36.	20(1)- Functions of the Board	Adding certain regulatory functions in addition to the adjudicatory functions may prevent the DPB from being treated as a tribunal, falling foul of Article 323-B of the Constitution.
37.	20(1)- Functions of the Board	Important functions such as notifying qualifications and certifying data auditors, prescribing the manner for data protection impact assessments, undertaking research, monitoring technological developments and raising awareness regarding the obligations and responsibilities under the DPDP Bill must be added to the DPB's functions.
38.	21(1)- Process to be followed by the Board to ensure compliance with the provisions of the Act	Redraft the provision to add clarity. Any techno-legal measures must be adopted by rules after consultation with the Supreme Court e-Committee. We recommend explicit exclusion of algorithmic adjudication of complaints.
39.	21(1)- Process to be followed by the Board to ensure compliance with the	Use of techno-legal measures must be accompanied by alternative modes for public-facing functions performed by such measures to avoid exclusion.

	provisions of the Act	Any digital mode of dispute resolution or adjudication must be voluntary and not mandatory.
40.	21(2)- Process to be followed by the Board to ensure compliance with the provisions of the Act	DPB must be given the power to *suo motu* take cognizance of violations of the DPDP Bill.
41.	21(4)- Process to be followed by the Board to ensure compliance with the provisions of the Act	A transparency obligation must be added to this provision such that reasons for closing proceedings on insufficient grounds are disclosed to parties.
42.	21(8)- Process to be followed by the Board to ensure compliance with the provisions of the Act	The DPB must be permitted to take into custody or otherwise restrict data in custody of data fiduciaries and data processors for at least six months to permit the DPB from carrying out their investigations regarding violations of the DPDP Bill.
43.	21(11)- Process to be followed by the Board to ensure compliance with the provisions of the Act	This provision must be omitted as levying a financial penalty only on significant violations of the Bill greatly harms the accountability and enforcement framework within the Bill, and creates room for arbitrary decision-making.
44.	24- Voluntary Undertaking	Voluntary undertakings must be limited to stages prior to issuance of notice for inquiry by the DPB under Clause 21.
45.	25- Financial Penalty	The DPDP Bill should include a penalty for re-identification of anonymised data.
46.	25- Financial Penalty	A provision that provides compensation to data principals harmed due to violations of the provisions of the DPDP Bill can be included.

Chapter 1: Preliminary

1. Definition of "Data Principal" (Clause 2(6))

Context: The definition provides that any individual to whom personal data relates to would be construed to mean a Data Principal, including the parents or lawful guardian of a child.

Issue: Extending the meaning of data principal to the parent/lawful guardian of a child would have a negative impact on the autonomy and informational privacy of the child. For instance, in the event that a data principal who is a child has sought assistance from an online social welfare portal due to abuse faced at the hands of a family member, this means that the parents of the child will also be able to access the personal data which the child has shared with the welfare provider/therapist.

Recommendation: In our view, the definition of Data Principal should be limited to "any individual to whom personal data relates to would be construed to mean a Data Principal". Alternatively, as will be discussed in relation with clause 10, the definition of "child" may be modified so that parental control does not apply to older children. Further, in this context, the clauses on data principal rights need to contain a requirement that data fiduciaries should not comply with a request for the exercise of such rights if such compliance would result in harming the rights of another data principal (here, the child herself).

2. Definition of "Harm" (Clause 2(10))

Context: The definition of harm in relation to a Data Principal is limited to bodily harm, distortion or theft of identity, harassment, prevention of lawful gain or causation of significant loss.

Issue: Limiting the meaning of harm to these factors may be too narrow to account for all types of harm that may be caused to a Data Principal. For instance, there are many types of harm that are intangible and may be difficult to quantify, but which are still detrimental to the Data Principal. The concept of harm is used in the DPDP Bill to identify significant data fiduciaries, undertake Data Protection Impact Assessments, and instructions by the Data Protection Board of India ("Board") in order to mitigate harm that may be caused due to a data breach.

Recommendation: The meaning of harm should be broadened in order to account for less tangible forms of harm, such as the potential for discriminatory action, exclusion, loss of reputation, chilling effects in speech etc. For this reason, the meaning of harm should include categories such as bodily or mental injury; loss of reputation; loss of employment; discriminatory treatment; being subject to blackmail or extortion; denial or withdrawal of service which may result from an evaluative decision being made about a data principal; and any restriction placed on speech or movement due to fear of being surveilled etc.

3. Definition of "Public Interest" (Clause 2(18))

Context: The definition of public interest has been defined as interest in the sovereignty and integrity of India; security of the State; friendly relations with foreign States; maintenance of public order; preventing incitement to the commission of any cognisable offence in relation to the above; and preventing the dissemination of false statements of fact.

Issue: There is an inconsistency between the above definition of public interest and the manner in which it has been utilised in the DPDP Bill. For example, reference to public interest has been made in four instances in this Bill. *First*, public interest has been referred to in Clause 8(8) under the "deemed consent" ground. This provision lists certain use cases where the personal data of a Data Principal may be processed without consent. Now, the use cases provided in Clause 8(8) appear to add several additional grounds under "public interest" which go beyond the scope intended within the definition of "public interest" in Clause 2(18). Clause 8(8) is thus inconsistent with Clause 2(18). For example, grounds such as prevention and detection of fraud, and credit scoring have nothing to do with the maintenance of the security and integrity of India. This inconsistency makes it unclear whether the term is in any way limited. *Second*, the definition of "public interest" allows for processing personal data for various purposes that are already listed as grounds for exemption under clause 18(2)(a) (integrity of India, public order etc.). There is no reason to duplicate the ground for exemption as grounds for processing except that it is made open to private persons. It would be entirely illegitimate for private persons to conduct national security and public order surveillance. *Third*, the only additional ground in the definition of "public interest" is for processing in order to prevent dissemination of false statements of fact. It is entirely unclear how this can be considered an adequate ground to allow for the violation of privacy when it is neither illegal to make false statements per se nor even a ground for the restriction of free speech. *Fourth*, the meaning of public interest is once again thrown open to interpretation in the manner that it is referred to under Clause 8(9) of the DPDP Bill, which provides that personal data may be processed under the deemed consent ground for any fair and reasonable purpose which may prescribed after taking into account any public interest which may exist.

Recommendation: The definition of "public interest" as well as clause 8(8) should be deleted altogether. The interests/grounds of processing listed in clause 8(8) may be retained as grounds with power to prescribe safeguards in relation with processing for any such interests.

4. Application of the Act (Clause 4)

Context: The provision provides for the applicability of the law and determines in terms of territorial and subject matter jurisdiction.

Issue:

1. The Bill appears to exclude offline personal data as well as non-automated processing from its remit under Clause 4(3)(a) and (b). This raises grave confusion as any non-automated processing of personal data is also certainly offline, in that any processing of personal data that is not undertaken without digitisation or automation would not have any connection with the internet, which is known to run on the basis of digital and automated means. Clause 4(3)(a) and (b) thus provides an incoherent picture as to what is intended to be left out of the scope of the law. This is aggravated further by

Clause 4(1)(a) and (b), which state that the Bill applies to "digital" personal data provided that it is either collected online or collected offline and then digitised. It is not clear what Clause 4(1)(b) refers to because "offline" collection can refer to both offline collection of non-digitised data (through analog means) or collection onto an offline computer directly (a computer not connected to the internet). The latter is already digitised at the moment of collection. Also in case of the latter, data would very much be offline (even if it is digitised) and it would thus meet the requirements of Clause 4(1)(b) but such offline data would then immediately be excluded from the applicability of the law under Clause 4(3)(b) simply by virtue of being offline (even if it is digitised). Clauses 4(1)(b) and 4(3)(b) appear to be in conflict with each other and the entire scheme of the clause is unclear as to whether only digital personal data is sought to be covered or online personal data.

2. If the intention is to exclude offline personal data (or offline personal data brought online), this is inadvisable as a wide variety of the most significant privacy harms may be caused while a computer is simply disconnected from the internet. This may also take place whether personal data is collected online and then brought offline or collected offline and kept offline (but in digitised form). It may also be an onerous task to determine what form of data has been collected online and it is entirely unclear as to how this would be proved for enforcement purposes.

Recommendation: The scope of the Bill must be clarified and rationalised to prevent inconsistent provisions. Given the practical and rights-based objections to an exclusion of offline data from the scope, the law should instead be made applicable to all digital personal data or processing through automated means (whether online or offline).

Chapter 2: Obligations of Data Fiduciary

1. Grounds for processing digital personal data (Clause 5)

Context: This clause states that a person may process personal data of a data principal only in the manner that is permitted under this Bill, and as long as such processing is performed for a lawful purpose for which a data principal has consented to, or which a data principal has deemed to give her consent. It is clarified here that a lawful purpose means any purpose which is not a person that has been expressly forbidden by law.

Issue:

1. Please note that this iteration of the DPDP Bill appears to have done away with several critical obligations in relation to data protection. For instance, this provision alludes only partially to the core principle of purpose limitation, it does away with the requirement that processing of personal data should be done for processes that are clear and specific as well as being lawful. The purpose limitation principle has been the bedrock of data protection regime.[1] It contains two sub-principles: first, that the purpose for which the

[1] See the EU GDPR, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013), FIPPs (FTC, US). See also Justice B.N. Srikrishna Committee of Experts, 'A Free and Fair Digital Economy Protecting Privacy Empowering Indians', p. 53.

personal data is processed must be clearly specified to the data principal (purpose specification); second, the processing must be limited to such purposes, or other compatible purposes (use limitation).[2] Further, purpose limitation is made meaningful only when a specific purpose is made known to the data principal *at the time of the collection of data* under the purpose specification principle. This obligation ensures the finality of the purpose and prevents subsequent changes, but it has been omitted.

2. The DPDP Bill also neglects to make mention of the collection limitation principle which mandates that only such data which is necessary for achieving specified purposes should be collected.

3. Failure to incorporate these principles may serve to dilute the autonomy and control that a data principal would be able to exercise over her personal data.

Recommendations: In our view, the grounds for processing personal data as currently mentioned under clause 5 should be further strengthened by also incorporating the principles of purpose limitation and collection limitation as mentioned above. This may be done by explicitly mentioning that purpose must be specified at the time of collection of personal data and that only such data be collected as is necessary for the specified purpose. The processing of personal data should also ordinarily be limited to the purpose that is specified at the time of collection and any limited deviation from the finality of the purpose specified in this manner should be clearly laid out in the law, for example through some principle of 'compatible' purposes where a new purpose has a strong relation with the purpose specified at the time of collection. Alternatively, the model adopted by some data protection laws (e.g. Canada and Singapore) is to limit processing to purposes that a reasonable person would consider appropriate in the circumstances. This would at least provide an intermediate level of purpose limitation.

2. Notice (Clause 6)

Context: This provision sets out the requirement for providing a data principal with notice before requesting a Data Principal for consent to process her personal data. It also mentions that the Data Fiduciary must provide Data Principals with notice for any processing which may be done before the commencement of this Act (once it is passed).

Issue:

1. The notice and choice framework is key to secure an individual's meaningful consent. While notice as an obligation plays an important role alongside consent, it also remains a crucial obligation even where processing takes place on the basis of grounds other than consent.[3] Where consent is not the ground (i.e. in the circumstances that the DPDP Bill refers to as 'deemed consent'), the provision of notice ensures that there is a specification of purpose at the time of collection and this ensures the meaningful implementation of purpose limitation. Without this, there is full freedom to alter purposes at any time after the collection as there would not be any sound method to

[2] Justice B.N. Srikrishna Committee of Experts, 'A Free and Fair Digital Economy Protecting Privacy Empowering Indians', p. 53
[3] Justice B.N. Srikrishna Committee of Experts, 'A Free and Fair Digital Economy Protecting Privacy Empowering Indians', p. 32.

determine what purpose was specified originally. It is necessary that such alterations in the purpose of processing be prevented or regulated in a systematic manner (e.g. as per specified exceptions in law or through the obligation of providing fresh notice when there is a change). This obligation is also required in ensuring that data processing is carried out transparently. Transparency is a key solution to the opacity of data processing and the amorphous nature of privacy harms.

2. Further, whether or not notice is given for consensual or non-consensual processing, the information provided must be adequate and should be retrievable subsequently from proactive disclosures related to privacy policies and standard form privacy notices. However, the provision in the DPDP Bill on notice only refers to disclosures on the description of personal data to be processed and the purposes of processing. Clause 7(3) separately requires disclosure of contact information on officers of the data fiduciary responsible. There are a variety of other points of information that should appropriately be disclosed including the permissibility of withdrawal of consent, the consequences of not providing consent, the source of collection, the entities with which data may be shared, the storage period etc.

Recommendations: Notice must be made mandatory even where there is a non-consensual round of processing. Suggestions on implicit consent under Clause 8(1) may be seen in the relevant portion below. Any exceptions from the obligation of notice must be limited by conditions of necessity or where the legitimate purpose of processing is made impossible to carry out by the provision of notice. The information provided at the time of notice must also be expanded, at least in the event that the notice is for sensitive personal data. Further, proactive disclosure of a privacy policy and the ordinary terms of data processing must also be provided for under the law.

3. Consent (Clause 7)

Context: Clause 7 states the conditions under which personal data may be processed on the consent of the data principal, putting in place requirements for the validity of such consent including that it must be free, specific, informed, unambiguous and capable of being withdrawn.

Issue:

1. The language of the provision indicates that certain fundamental aspects of consent as a ground of processing personal data have been misunderstood. Specifically, the ground of consent has been confused with contractual processing. *First*, sub-clause (2) invalidates any consent that is violative of provisions of the law and provides contractual waiver of data principal rights as an illustration of invalid consent. To start with, the provision is incorrectly framed as the waiver of statutory rights is not per se an "infringement" of the Act. The situation mentioned in the illustration is thus not addressed by the provisions itself. More importantly, however, the ground of consent is conceptually distinguished from contractual processing on the basis that consent is not given for consideration as otherwise this allows personal data to be made into "counter-performance" i.e. it allows persons to pay for goods and services with personal data. There are significant problems

with permitting such contractual behaviour.[4] *Second*, this Bill continues the error made by the 2019 Bill in stating that the consequences of withdrawing consent would be borne by the Data Principal. The 2018 Draft Bill had attempted to clarify that only a specific kind of withdrawal of consent would face this repercussion: "consent for the processing of any personal data necessary for the performance of a contract". This formulation attempted to differentiate consent outside of a contract from consent that is part of a contract because consent for personal data (being freely withdrawable) is not meant to be given in payment for services but data may be used insofar as it is *necessary* for the performance of a contract.[5]

2. A further omission in the provision compared to analogous provisions in previous versions of the Bill is in relation with what may be called 'bundling' or 'tying up' consent with other grounds of processing. Sub-clause (8) correctly identifies that the performance of a contract should not be made conditional on giving consent for data that is not necessary for such performance, but the same conditionality should also be avoided when providing for the enjoyment of rights. If certain data is not necessary in allowing the data principal to enjoy social welfare rights, the provision of these rights must not be held hostage when demanding for consent. Such grant of consent would not be freely given and such conditionality deserves to be explicitly prohibited.

Recommendation: In relation with sub-clause (2), if the concern mentioned in the illustration is the main objective, it may be addressed by creating a separate provision disallowing the waiver of data principal rights. This may be done for caution even though such waiver may be illegal under the doctrine of waiver. In sub-clause (4), the provision for "consequences" of withdrawal of consent should be restricted to consent for processing personal data necessary for the performance of a contract. In sub-clause (8), making the enjoyment of rights conditional on grant of consent not necessary for the provision of those rights should be explicitly prohibited.

4. Implicit/Deemed Consent (Clause 8(1))

Context: Sub-clause (1) of clause 8 sets out certain conditions under which the data fiduciary does not have to meet the higher standard of specific, unambiguous and withdrawable consent provided in clause 7 and can process personal data on a lower standard of implied consent. The conditions for such implied consent are that it must involve a voluntary provision of personal data where such provision is reasonably expected.

Issue: This provision dilutes the protection for personal autonomy granted under clause 7. A data fiduciary would be able to process every kind of personal data (including sensitive personal data) on meeting simple and undemanding conditions. *First*, processing is made permissible not when there is some affirmative action providing consent but merely when there is some voluntary action that 'provides' the data. The term 'provide' includes the action of

[4] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content' (14 March, 2017); European Data Protection Supervisor, 'Opinion 8/2018 on the legislative package "A New Deal for Consumers"' (5 October 2018)
[5] The intention behind the provision is discussed in Justice B.N. Srikrishna Committee of Experts, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians', pp.38-42

simply making something available,[6] which may be done without any affirmative action and simply by becoming observable or making the collection of data possible by visiting a place (with a CCTV camera, for example) or a website (that collects device-specific data). The word 'voluntarily' may seem to limit what data may be processed but this would not make much of a difference since one can freely expose oneself and make data available without ever agreeing to its collection or use. *Second*, the additional requirement is that the provision of data must be reasonably expected. Once again, one may reasonably expect that data is made available without meaningfully consenting to its collection and use. This is a weakness inherent in the 'reasonable expectation' theory of privacy, which is circular in that it depends on the expectations created in society rather than creating legal standards on voluntariness that set new expectations.[7] *Third*, the provision refers only to reasonable expectation of the provision of data and makes no mention of the purpose of its usage. The illustration refers to the concept of purpose but this would not change the content of the sub-clause itself. The failure to mention anything along the lines of reasonable expectation of a purpose of usage means that there is no limitation on the *purpose* for which the data may be used at all, only that its *provision* should be reasonably expected. A limitation on provision or collection is not a limitation on usage. *Fourth*, the provision seems to exclude the possibility of withdrawal of consent. It is inconsistent that there should be provision for withdrawal of consent when it is explicit but no provision for such withdrawal when it is implicit. The likelihood that data provided voluntarily would cease to enjoy the approval of the data principal is higher in the event that the consent was implied or ambiguous, especially if she later learns the full implications of this 'consensual' provision of data. As a result of the scheme of this sub-clause, the requirement of explicit consent with notice (under clause 7) would be applicable only in the limited circumstance where provision of personal data is not reasonably expected.

Recommendation: This clause should be deleted as it significantly dilutes provisions in the Bill aimed at bolstering personal autonomy. Consent should ordinarily be a ground for processing personal data only if some affirmative action is made to provide it and this has been revealed in the course of long experience of jurisdictions like the EU dealing with data protection law. Various circumstances where reasonable expectation may be at play should be dealt with under fair and reasonable expectations on carrying out a balancing exercise. Alternatively, the provision should contain further strict conditions:

(a) Consent for processing personal data must be for a fixed purpose, even if such consent is implied;
(b) Implied consent should be withdrawable;
(c) It should be impermissible to use implied consent to process sensitive personal data or process any personal data in a way that may cause a risk of significant harm; and
(d) Further guidance may be provided on when consent may be implied for contractual necessity or on the provision of some form of notification.

For the phrasing for such stricter provisions, the provisions on implied consent in the data protection laws of Canada and Singapore may be seen.[8]

---

[6] Merriam-Webster Dictionary, 'Provide', available at <https://www.merriam-webster.com/dictionary/provide> (last accessed 16th December, 2021).
[7] It may be noted that one of the judges in *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 rejected the applicability of this test (Nariman, J. at para.494).
[8] S.6.1 and Paragraph 4.3 of Schedule 1, Personal Information Protection and Electronic Documents Act, 2000 (Canada); Ss.15 and 15A, Personal Data Protection Act, 2012 (Singapore).

5. Non-Consensual Processing (Clause 8(2)-(8))

Context: Sub-clauses (2) to (8) of clause 8 provide for various instances under which personal data may be processed without the actual consent of the data principal and it is phrased as involving the deemed consent of the individual.

Issue: The phrasing of these provisions as 'Deemed Consent' is incoherent and likely to result in considerable confusion. This is particularly because sub-clause (1) of clause 8 is already phrased in a way that is closest in meaning to the legal concept of 'implicit' or 'deemed' consent. Placing additional grounds for processing personal data non-consensually within the same umbrella fails to account for the critical differences between these additional grounds and the implied consent in sub-clause (1). This includes the question of withdrawal of consent which must be permitted for processing under sub-clause (1) but would not be meaningful in relation with the latter seven grounds of 'deemed consent'. What is more, it is not meaningful to refer to these grounds of processing data under the rubric of 'consent' as they are grounds where processing is to take place regardless of whether there is any real voluntariness on the part of the data principal. There is no consent envisaged in such instances, whether explicit or implied. Referring to these situations as involving something that should be 'deemed' as being 'consent' or where there should be a legal fiction that there is consent suggests that the law should treat these situations as involving consent.

Recommendation: Sub-clauses (2) to (8) of clause 8 should be separated from sub-clause (1) and placed in a separate provision that is distinct from the concept of deemed consent and referred to as non-consensual grounds of processing.

6. Performance of functions of the State (Clause 8(2))

Context: This provision permits processing of personal data by the State in three situations: 1. for the performance of any function under any law; 2. the provision of services of benefits to the data principal; and 3. issuance of permits to the data principal.

Issue: *First*, the processing permitted under this provision in the second and third situations mentioned above do not require authorisation of the law. This is made permissible particularly because it is implied by the absence of "under any law" which is only mentioned in relation with the first situation. The processing of personal data by the State for the provision of services and issuance of permits cannot be permitted without authorisation of a law as this would violate the first requirement of 'legality' under the proportionality test applicable for the right to privacy.[9] *Second*, processing under this provision is permitted for State instrumentalities even if they are not carrying out any State function. Thus, State instrumentalities like government companies or any other entity providing goods or services as a business enterprise is permitted to process personal data without consent even though consent, contractual necessity or reasonable purposes is the appropriate ground for processing where a business

[9] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1, at para.325 (Chandrachud, J.).

activity is being undertaken. It would be irrational to permit government companies to process under less restrictive conditions than private companies.

Recommendation: The requirement of authorisation of law must be placed on any processing for provision of services or benefits and on processing for issuance of permits. Further, processing under this provision should only be for functions of the State or should at least exclude business activities.

7. Compliance with law (Omitted)

Context: There is no provision in the Bill for processing of personal data necessary for compliance with the law. Such a provision may, for example, be seen at clause 14(a) of the 2018 Draft Personal Data Protection Bill.

Issue: Where any private person is required to process personal data to comply with a law, such processing would be illegal under this Bill. Such processing seems to be referred to and permitted under Clause 7(5), but this is not accounted for within the binary of consent and deemed consent as grounds for processing under Clause 5.

Recommendation: The appropriate placement for a ground for processing in compliance with a law is within the list of non-consensual grounds. It should be reintroduced there.

8. Employment Purposes (Clause 8(7))

Context: This provision permits processing of personal data for 'purposes related to employment' and lists certain examples of these purposes.

Issue: The provision is open-ended in its phrasing and allows for non-consensual processing for various purposes merely because they are necessary for purposes 'related' to employment. It is not clear what kind of relatedness with employment would bring matters within this ground. This is aggravated by the fact that various purposes listed as examples include prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, and classified information. These are all instances of requirements of legal confidentiality or intellectual property rights of businesses, corporations, or other juristic persons. They may be valid grounds for the prosecution of a person violating contractual or statutory rules on confidentiality, but they are in no way valid grounds for the violation of privacy of individuals who may or may not be engaging in such illegalities. What is more, a ground on processing for employment purposes requires safeguards including an obligation to opt for consensual processing where this is appropriate and feasible.

Recommendation: This provision should be restricted to listed employment purposes instead of being made open ended. Purposes related to confidentiality and intellectual property rights must be excluded entirely from this closed list. Safeguards must be introduced to ensure that this ground may only be employed where obtaining the consent of an employee is appropriate and feasible.

9. Public Interest and Fair and Reasonable Purpose (Clause 8(8) and (9))

Context: This provision lists various purposes for which personal data may be processed, including prevention and detection of fraud, network and information security, credit scoring, processing of publicly available personal data etc. It refers to all of these purposes as being in "public interest", a term that is defined in clause 2(18).

Issue:

1. As discussed in relation with the definition of "public interest" in clause 2(18), the purposes listed in that definition and the purposes listed as examples in clause 8(8) are inconsistent with each other. The purposes listed as examples in clause 8(8) may be appropriate grounds for processing personal data non-consensually only if they are appropriately restricted with adequate safeguards. For example, the mere fact that personal data is available publicly should not permit a data fiduciary from using that data in ways that might harm the data principal, not least because data may have become publicly available in various illegitimate ways. Similarly, personal data may be processed in harmful ways that are claimed to be "necessary" for recovering debt but are nonetheless disproportionate. This should be limited with safeguards.

2. The ground of "fair and reasonable purposes" in sub-clause (9) should not be directly available to the State or State instrumentalities as such entities must process personal data on the authorisation of a law that governs processing in relation with the relevant matters (as discussed in relations with clause 8(2) above). The same should be applicable to the grounds referred to in sub-clause (8) under "public interest".[10]

Recommendation: The purposes listed in this sub-clause should not be referred to as "public interest" due to inconsistency with the definition of that term. Insofar as they are grounds to permit the use of personal data without consent, they should be restricted with adequate safeguards that prevent disproportionate invasions into the rights of individuals or the risk of significant harm. These safeguards may be adapted in due course of time with appropriate rules or regulations. The guidance for the prescription of these safeguards may be similar to the criteria listed for 'fair and reasonable purpose' under sub-clause (9). Appropriately, it may be combined with sub-clause (9) as retained in previous versions of the Bill. The moniker of "fair and reasonable purpose" or "legitimate interest" would provide better guidance and precedent rather than "public interest". Sub-clauses (8) and (9) should not be available to State entities without authorisation of a law on the specific grounds and this may be stated explicitly within this clause.

10. General Obligations of Data Fiduciaries (Clause 9)

Context: This provision lists out the general obligations that must be followed by data fiduciaries when they process personal data whether on the ground of consent or deemed

[10] This distinction may be seen in the EU GDPR (see Article 6(1) and Recitals 45 and 47).

consent. These obligations include the maintenance of the accuracy of data, implementation of technical and organisational measures as well as security safeguards, actions to be taken in the event of a data breach, storage limitation measures etc.

Issue:

1. Under sub-clause (4), the data fiduciary is required to implement reasonable security safeguards to protect the personal data in its possession. This obligation is already limited by a requirement of reasonableness but it is further limited because the provision states that such safeguards are only aimed at preventing data breaches. If there is no risk of a data breach, then the fiduciary need not implement security safeguards. However, security safeguards do need to be implemented to secure personal data from privacy harms other than data breaches. As per clause 2(14), data breaches are limited to unauthorised and accidental activities that compromise the confidentiality, integrity or availability of data. However, in certain circumstances, security measures such as de-identification and encryption are reasonable safeguards for protecting privacy. Such measures secure data even when the processing undertaken is authorised and intentional. Security safeguards ensuring the continued integrity or quality of data would also be necessary even where there is authorised and intentional processing.

2. Under sub-clause (6), a general obligation is placed limiting the retention or storage period for personal data. Under this obligation, data that is no longer needed for the purpose for which it was collected is required to be deleted. This is partly recognised under paragraph (a) of sub-clause (6) (though the absence of a proper purpose limitation provision in the Bill militates against this). However, the finality of the determination of this purpose (set at the time of collection) is deviated from by referring to storage for additional "legal or business purposes" as per paragraph (b). While it is noted that this phrasing is borrowed from the Singaporean Personal Data Protection Act, 2012, there are risks that this phrasing is too broad an exception from ordinary norms of storage limitation. To start with, it is not clear what kind of business purposes a data fiduciary may continue to store data for, and this may simply mean profit-making purposes. It is similarly unclear whether this permits the retention of data for purposes other than those authorised under clauses 7 and 8 (on consent and deemed consent).

3. Sub-clause (9) refers to two distinct subject matters: the transfer of personal data by one data fiduciary to another, and the engagement of a data processor to process data on behalf of a fiduciary. In relation with the first, the provision makes it appear that personal data may only be transferred by one data fiduciary to another on the ground of consent. If this were not its meaning, the reference to transfer/transmission in this provision would be redundant. However, data fiduciaries are required to transfer data to other fiduciaries on various non-consensual grounds that could include compliance with law, State functions, contractual necessity, or a fair or reasonable purpose. Further, the phrasing of this provision makes it unclear whether the permissibility of engaging a data processor is also limited only to circumstances where the consent of the data principal is obtained.

Recommendation: The obligation of reasonable security safeguards should be extended beyond prevention of data breaches and should cover safeguards related to de-identification, encryption and data integrity. The obligation on storage limitation must limit the exception from purpose limitation to only those legal and business purposes that are legitimate or otherwise covered under grounds of processing, and any such exception should be made justifiable with provision of notice where applicable.[11] The two subject matters covered under sub-clause (9) should be separated into different sub-clauses to prevent confusion. Transfer of data from one data fiduciary to another should be permissible so long as it is necessary under one of the grounds of processing under Clauses 7 and 8.

11. Additional obligations in relation to processing of personal data of children (Clause 10)

Context: This provision specifies on how the personal data of children should be processed.

Issue:

1. The DPDP Bill, like the previous iterations of the law, treats any data principal below the age of 18 to be a child. This construction is problematic because it does not take into consideration that a "child" who is a toddler and a "child" who is a teenager are at very different stages of emotional and intellectual development. The determination of a suitable age while deciding who should be considered a child varies greatly among data protection laws across various jurisdictions. For example, in the United States of America, the Children's Online Privacy Protection Rule ("**COPPA**") allows children 13 years of age and above to consent, whereas Article 8 of the EU GDPR mandates age 16 as the threshold, though allowing leeway for member states to reduce the age of consent to 13. The factors in determining the cut-off age of children are commonly recognised to be on the basis of certain principled considerations and that the age range should ideally be between 13 and 18, as well as ensuring that the threshold is practical to implement by data fiduciaries.

2. Having a single threshold of 18 is problematic because this would mean that the consent of the parent or guardian would be required every time the data principal (child) wishes to access any website/ any service which would require the processing of her personal data. This would have the detrimental effect of affecting autonomous development of the child or teenager. This is also in violation to the CRC.

3. Further, being able to develop a fool-proof mechanism to verify the parent or guardian of the child by all data fiduciaries would result in being a compliance burden, not to mention the difficulty of developing such a system at all.

4. In addition, as discussed above, by including the parents/guardians of a child within the definition of a data principal would have the effect of further diluting the rights of the child as a data principal. In the event that a child was seeking either counselling help, or

[11] Graham Greenleaf, *Asian Data Privacy Laws: Trade & Human Rights Perspectives* (2014), p.302 (discussing Singapore's data retention obligation).

trying to access resources that would provide assistance in situations like domestic abuse or child abuse (perhaps within the family itself), then seeking the consent of the parent or guardian would defeat the purpose.

Recommendation:

1. It is recommended that the age of a "child" be reduced to below 18.

2. The definition of data principal should not extend to the parents and guardians of a child.

Chapter 3: Rights & Duties of Data Principal

1. Right to information about personal data (Clause 12)

Context: The DPDP Bill provides that the data principal shall have the right to get certain information from the data fiduciary.

Issue: In the absence of a comprehensive notice, the categories of information listed under Clause 12 form the mainstay of information that a data principal can access. While the fields of information are adequate, and expandable if the Rules so provide, the clause omits the obligation to provide this information in a clear and comprehensible manner to the data principal. This is a crucial omission. Access to clear, concise and comprehensive information is the foundational right for accessing other rights of the data principal. As such, the manner of information provisioning is as crucial as the nature of information.

Recommendation: Right to information should incorporate the obligation on the data fiduciary to provide the specified information in a clear, concise and comprehensible manner to the data fiduciary.

2. Right to correction and erasure of personal data (Clause 13)

Context: The DPDP Bill provides the data principal the right to correction and erasure of personal data.

Issue:

1. "in accordance with the applicable laws": Clause 13 requires correction and erasure of personal data be made "in accordance with applicable laws". It is unclear what this addition means considering that any exercise of power under the law has to be in accordance with the applicable laws. It is possible that this reference to the exercise of this right "in accordance with the applicable laws" could be an attempt to accommodate the right to be forgotten which has not found an express mention in the DPDP Bill. However, if that is the case, the current drafting of this clause may be too overbroad and an overreach to achieve the right to be forgotten. A request for the erasure of personal data may, in particular, have significant effects on the right to information and the right to free speech and expression, and any provision that allows for the right to erase

published or shared data must take into account that privacy must be balanced in such circumstances with such conflicting rights.

2. Clause 13(2)(d) provides that a data principal can request for erasure of their personal data when the personal data is no longer necessary for the purposes for which it was processed unless it is not required to be retained for a legal purpose. This is in conflict with clause 9(6) of the DPDP Bill which allows data fiduciaries to retain personal data for "business purposes" also. This would mean that the data principal's request for erasure of personal data can be rejected if the data fiduciary wants to retain personal data for "business purposes".

3. The current formulation does not specify how a conflict between the data principal and data fiduciary will be resolved in case of disagreement between them on whether the personal data is to be corrected or erased.

4. There is no express obligation on the data fiduciary to pass on the corrections or updation made or any erasure that has happened to third parties with whom the data fiduciary has shared this personal data.

Recommendation:

1. To avoid confusion over the scope of "applicable laws", it would be useful to separately provide for the right to be forgotten within the DPDP Bill. Such express mention would help in including considerations of right to information and freedom of speech and expression while considering whether information needs to be erased.

2. There needs to be reconciliation on the grounds on which correction and erasure can be requested and the purposes for which the data fiduciary can retain personal data. For comments on retention of personal data for "business purposes", please refer to our submissions on the subject in relation with chapter 2 above.

3. There needs to be a conflict resolution mechanism in case the data fiduciary disagrees with the data principal's right to correction and erasure of personal data. This could be done by way of approaching the grievance redressal mechanism of the data fiduciary and marking personal data over which such disagreement has arisen.

4. The data fiduciary should also be obligated to pass on any information that it has corrected, updated or deleted to the relevant third parties it may have shared this personal data with. This flows from the understanding that data protection obligations run with the data, and are not limited to the first incidence data fiduciary with which such data has been shared.

3. Right of grievance redressal (Clause 14)

Context: The DPDP Bill provides the data principal the right of grievance redressal.

Issue: Clause 15 only specifies that the data fiduciary should provide for "readily available means" for registering a complaint with the data fiduciary. It fails to provide further specifications on the design of grievance redressal. While this may have been done to allow data fiduciaries to come up with customised designs for grievance redressal, it also allows data fiduciaries to completely obviate the need of a human element in resolution of grievances and make it completely dependent on automated processes. This especially so given the shortened timeline for dispute resolution i.e. seven days from the date of registration of the complaint. Such complete reliance on automated processes may lead to unsatisfactory resolution of the grievance. While clause 15 provides that the data fiduciary may approach the Data Protection Board of India (DPB) in case of unsatisfactory resolution, this may not be an adequate design given that it will either lead to excessive number of complaints being filed with the DPB or may deter data principals from utilising the grievance redressal due to repeated unsatisfactory resolution.

Recommendation: The DPDP must mandate some form of human interface in the grievance redressal mechanism of the data fiduciary.

4. Right to Nominate (Clause 15)

Context: Data principals may nominate another individual who may exercise the rights of the data principal on their behalf, in the event of death or incapacity. Here, incapacity is defined as the inability of a data principal to exercise their rights under this act due to unsoundness of mind or body.

Issue: While the right to nominate is a positive inclusion for the rights of the data principal, the nomination gets triggered in the event of death or incapacity for the data principal. While the concept of unsound mind is understood in Indian jurisprudence under Section 12 of the Indian Contract Act, 1872, the rationale behind unsoundness of body as a form of incapacity is unclear.

Recommendation: If the intent of the legislation is to offer the benefits of nomination in the event of total bodily disability, that should be clarified in the text. In its current iteration, the threshold to what constitutes an unsound body is unclear and may be misused.

5. Duties of data principals (Clause 16)

Context: This provision sets out certain duties applicable to data principals. These duties include compliance with applicable laws, and prohibits registering false complaints with the data fiduciary or the DPB, furnishing false particulars or suppressing material information while applying for any service, unique identifier or proof of identity.

Issue:

1. This provision is over-broad and extremely prone to misuse. The requirement to abide by applicable laws while exercising rights under this Bill is wholly unnecessary. For external

laws, violations of those obligations are appropriately punished under those laws. Additionally, the objectives of such a provision are unclear. Clause 16(1) does not add any additional duty. Clauses 16(2), 16(3) and 16(4) create certain obligations on the data principal, a failure of which is punishable under Clause 21(2) of the DPDP Bill read with Clause 25.

2. Clause 16(2), read with Clause 21(2) of the Bill, may result in financial penalty being levied on data principals for filing a false or frivolous grievance with the data fiduciary or the DPB. Data principals may file grievances for a variety of reasons, including the fact that they are not aware of, and are unable to access, the correct information or the correct status of their personal information with a data fiduciary. In such cases of information asymmetry, certain complaints may ultimately end up being 'false'. Additionally, what may seem 'frivolous' for a data fiduciary or the DPB may not be frivolous for a data principal, moreover so if the data principal is entitled under the DPDP to file such a complaint.

3. In Clause 16(3), the language reads "*Data Principal shall, under no circumstances <u>including</u> while applying for any document, service, unique identifier, proof of identity or proof of address, furnish any false particulars or suppress any material information or impersonate another person.*" The obligation to not submit false particulars or suppress material information is necessary in the context of authenticating oneself to receive certain services or apply for certain government documents. However, this provision suffers from a drafting error by using the word 'including', thus expanding the obligation of not furnishing false particulars or suppressing material information to scenarios beyond the specified examples mentioned in the provision.

<u>Recommendation</u>:

1. We recommend that Clause 16(1) be omitted from the drafting of this Bill. The inclusion of Clause 16(1) does not serve any purpose under the DPDP Bill other than to reiterate the existing obligations under Clause 16. Further, by imposing an obligation on the data principal to comply with provisions of 'all applicable laws' while exercising rights adds to the confusion to data principals. Making the rights of data principals conditional on compliance with all applicable laws defeats the purpose of those rights being inherent to the right to privacy, and leaves the door open for misuse against those seeking to exercise their rights.

2. In these circumstances, creating a duty to not file false or frivolous complaints, and making violations of this duty punishable by a financial penalty, may impose grave chilling effects. We recommend that this provision be omitted as furnishing any false information within a complaint is already covered under Clause 16(3), and punishing 'false' or 'frivolous' complaints may punish complaints filed by data principals without any malice or intent to deceive the data fiduciary or the DPB.

3. The use of the word 'including' makes it a duty of the data principal to never, under any circumstance, furnish false particulars or suppress material information for any action

whatsoever, including the few scenarios mentioned in the provision. However, this cannot become a general obligation across the internet. Data principals, as users of digital services, continue to retain the right to anonymity in their personal interactions with such services. Mandating that all material information be shared for all actions online effectively removes the 'right to be left alone' for personal interactions, which is a core component of the right to privacy under *KS Puttaswamy v Union of India*.[12] Accordingly, we recommend that the word 'under no circumstances including' be replaced with 'not'. Additionally, the obligations set out in Clause 16(3) must be limited to obtaining documents, services, unique identifiers, proof of identity or address from state institutions. Actions of the data principals outside these services must be left to private parties, including the users and providers of digital services to preserve the right to online anonymity.

Chapter 4: Special Provisions

1. Transfer of personal data outside India (Clause 17)

Context: The DPDP Bill allows data fiduciaries to jurisdictions notified by the central government.

Issue:

1. Clause 17 of the DPDP Bill does not clarify whether there is a prohibition on transferring personal data to any other country unless it has been notified by the central government. This raises the question of whether there is a *de facto* data localization and non-sharing requirement for all personal data unless specific countries have been notified as permitted territories. The provision, as it is currently framed, seems to prohibit the transfer of personal data to any country not notified by the central government.

2. The DPDP Bill fails to provide any factors that the central government should consider while notifying jurisdictions where transfer of personal data is allowed. This suffers from excessive delegation. The absence of criteria is further problematic as it could create apprehension in the minds of data principals on whether the jurisdictions where their personal data is being transferred adhere to sufficient data protection safeguards. This is especially so because the DPDP Bill allows cross border transfer of sensitive personal data without the explicit consent of the data principals.

Recommendation:

1. As the current draft seems to implicitly prohibit transfer of personal data by data fiduciaries to any country unless it is notified, which is an obligation on data fiduciaries and is better placed within Chapter 2, we recommend that the provision be redrafted to reflect the intent of this provision, to avoid confusion regarding obligations of data fiduciaries.

[12] (2017) 10 SCC 1

2. The DPDP Bill should provide a list of indicative, if not, exhaustive criteria which the government would consider in notifying the relevant jurisdictions. These factors could include considerations of equivalent data protection obligations in the jurisdiction and the impact that this transfer could have on the enforcement of relevant laws by authorities in India. Further, the jurisdictions notified should be under periodic review.

2. Clause 18- Exemptions

Context: This provision sets out various clause-specific and entity-specific exemptions from provisions under the DPDP Bill.

Issue:

1. The exemptions provided under Clause 18(1)(c) are currently too broad, and are not limited to state agencies. Under the current framing of this provision, wide-ranging exemptions from Chapters 2 and 3 can be claimed even by private data fiduciaries processing personal data for prevention or detection of offences. State agencies carrying out law enforcement must also be subject to the requirements of proportionality or else their activities would be in violation of the right to privacy under the Constitution.

2. The exemption under Clause 18(1)(d) is neither phrased appropriately nor advisable given its likely effects. As currently phrased, the provision exempts the personal data of persons not within the territory of India. It may be noted that this even includes residents and citizens of India who happen to be abroad for the duration of their travel, even if their data never left India. It is unlikely that this is the intended effect of the drafting but it is the meaning of the language employed. It is thus unclear what is being referred to in this provision: data that is collected/processed outside the territory of India or data of non-residents. If it is the former, then the matter should be addressed under clause 4(2) which deals with extraterritorial applicability of the law. If it is the latter, it may be noted that it is notoriously difficult to establish where a data principal is resident in the context of the internet and this is likely to result in confusion at the time of compliance. More importantly, the exemption of the data of non-residents from any data protection obligation is likely to result in the inability of India to meet the requirements for 'adequacy' as determined by the EU as well as similar tests for the transfer of personal data to India. Just as significantly, it may be noted that such an exemption would make an unjustified distinction between citizens and non-citizens and make the exemption vulnerable to being struck down as unconstitutional for violation of Article 14 and Article 21 (under which the right to privacy would extend to non-citizens as well).

3. While permitting the central government to exempt any notified 'instrumentality of the State' from their obligations under this act for certain grounds, Clause 18(2)(a) does not limit this exemption to necessity and proportionality as held by the Supreme Court in *KS Puttaswamy v Union of India*.[13] Additionally, this provision requires no alternative

[13] (2017) 10 SCC 1

procedures, timelines or safeguards to be committed to by the instrumentality being exempted under the specified grounds.

4. Clause 18(2)(b) permits the central government to exempt any personal data processing necessary for research, archival or statistical purposes. This exemption is only conditional on the standards which shall be specified by the DPB and that the personal data shall not be used to make any decision specific to a data principal. However, this provision fails to include appropriate safeguards for the protection of data principals. It creates a very low bar for personal data to be processed by data fiduciaries for research purposes, removes accountability from basic obligations of lawful purpose, security standards, notification on data breach, appointment of a data protection officer and storage limitation. The purpose for providing such wide-ranging exemptions for research, archival or statistical purposes is not clear, and may not withstand a constitutional challenge. Further, it denies data principals from any recourse to their rights under the DPDP Bill in the event of misuse or failure to protect personal data by the data fiduciary.

5. Under Clause 18(3), the central government may notify certain data fiduciaries from clauses 6, 9(2), 9(6), 10, 11, and 12 of the Bill. We note that Clause 10(4) currently permits the central government to exempt the provisions of Clause 10(1) and Clause 10(3) for certain purposes. Further, we note that the obligations under Clause 11 are only applicable to data fiduciaries notified by the central government as significant data fiduciaries. Accordingly, notifying data fiduciaries exempted from the obligations under Clause 11 seems redundant.

6. Under Clause 18(4), all state instrumentalities are exempted from the obligation of storage limitation under Clause 9(6). The purpose sought to be achieved by such an exemption is unclear. Permitting such a wide-ranging exemption for any instrumentality of the State is not in line with the objectives of this legislation, and in our view, would be ruled as unconstitutional as it fails the test of reasonable classification under Article 14 as well as the right to privacy as applicable to the State. There is no rational nexus between the distinction of state and non-state entities and the objective of limiting the duration of data storage as the State has no special interest in maintaining continued storage of personal data beyond the period required for the functions of the State. What is more, the Supreme Court has explicitly required strict storage limitation obligations for State entities in its 2018 judgement on informational privacy in the context of the Aadhaar legislation.[14] There is ample reason to ensure that the State adheres to the principle of storage limitation if it is to avoid the charge of unconstitutionality in its data processing activities.

7. We note that Clause 18 does not provide any exemptions for processing of personal data for journalistic purposes or for literary, academic or artistic expressions. This is a widely prevalent exemption to the right to privacy and data protection, in order to balance it with the right to free speech and expression.[15]

[14] *KS Puttaswamy v Union of India* (2019) 1 SCC 1, paras 205, 284, 447(4)(c)
[15] Article 85, General Data Protection Regulation 2016; see also Part 5, Schedule 2 of the UK Data Protection Act, 2018

Recommendation:

1. We recommend that the exemptions available under 18(1)(c) must be provided in a qualified manner and must be limited to state agencies, keeping in mind the nature of exemptions provided to any private entity such as malls or shopkeepers placing closed circuit camera televisions in public places. Further, any exemption granted to state agencies carrying out law enforcement must also only be granted if those agencies otherwise adhere to substantive and procedural safeguards that meet the test of proportionality.

2. It is unclear what is intended to be exempted under clause 18(1)(d), but even if the intention is to exempt the personal data of non-residents, the provision deserves to be deleted.

3. We recommend that Clause 18(2)(a) specify that the exemptions provided to state instrumentalities be limited to such exemptions as are necessary and proportionate, in accordance with *KS Puttaswamy v Union of India*. Further, we recommend that any exempted instrumentality be required to set out timelines for the exemptions as well as safeguards and oversight mechanisms operating on the actions of the instrumentality during such exemption.

4. Adding certain safeguards to limit the instances where such wide-ranging exemptions may be granted creates a less restrictive and proportionate manner in which personal data is processed for research, archival or statistical purposes. We recommend that the safeguards include only granting such exemptions only if compliance with the provisions of the DPDP Bill renders impossible or seriously impairs these purposes. Further, processing personal data under this provision must not be permitted if there is a chance of significant harm to the data principal. Lastly, we recommend that certain provisions, such as Clause 4 and Clause 9, must not be exempted for data fiduciaries acting under this clause.

5. We recommend that any exemptions from Clause 10 from the obligation of data fiduciaries based on volume and nature of personal data processed be shifted to Clause 10, instead of a separate sub-clause under Clause 18. Further, we recommend omitting the reference to Clause 11 from Clause 18(3).

6. We recommend that this provision be omitted from the draft DPDP Bill.

7. We recommend the addition of certain exemptions missing from the DPDP Bill, such as processing personal data for journalistic purposes and for literary, academic or artistic expression, in order to reconcile the right to privacy with the right to free speech and expression guaranteed under Article 19(1)(a) of the Constitution.

Chapter 5: Compliance Framework

1. Data Protection Board of India (Clause 19)

Context: The DPDP Bill sets out the DPB as the nodal agency responsible for ensuring compliance with the provisions of this Act, and to adjudicate and penalise violations of this Act.

Issue:

1. Digital by design: Under Clause 19(1), the DPB shall be 'digital by design' for its functions such as allocation of work, receipt of complaints, formation of groups for hearing, pronouncement of decisions, and other functions of the Board. Mandating public-facing functions of the DPB such as the receipt of complaints be handled in a 'digital by design' manner is inadvisable. This may exclude several data principals who do not have reliable digital means of pursuing their rights under the DPDP Bill.

2. Independence of the DPB: Clause 19(2) does not provide any guidance regarding the constitution of the DPB, and states that the strength, composition, selection, terms and conditions of appointment and service, and removal shall be further prescribed in rules. This clause does not provide enough clarity regarding the need for institutional or functional independence of the DPB for future subordinate legislation.

Recommendation:

1. While the DPB's internal functioning can be carried out through a 'digital by design' mandate, its public-facing functions such as enforcement of data principals' rights, receiving complaints and hearing parties in the course of its adjudication. We recommend that Clause 19(1) be redrafted with an explicit requirement for the DPB to provide equally effective alternative means for its public-facing functions to address issues of exclusion for such scenarios.

2. The DPB serves a judicial role under the DPDP Bill and is therefore a quasi-judicial body. The Bill itself does not offer any clarity regarding the institutional independence of the DPB, i.e., degrees of separation from other branches of the government, or regarding the functional independence of the DPB, such as the methods of selection and removal and ensuring decisions are free from executive pressure. We recommend that Clause 19 be redrafted to offer statutory safeguards for both functional and institutional independence of the DPB, which can then determine the nature of subordinate legislation for these matters.

2. Functions of the Board (Clause 20)

Context: The clause sets out the function of the proposed DPB, which are to ensure compliance with the provisions of the DPDP Bill.

Issue:

1. Lack of clarity over the role and functions of the DPB: Under clause 20 (1)(a) of the DPDP Bill, the main function of the DPB is to "determine non-compliance of the Act and impose penalty" in accordance with Schedule 1. While sub-clause (b) allows for the

Central Government to add more functions, presently the role of the DPB is akin to a *quasi-judicial* tribunal adjudicating complaints. This understanding is corroborated by recent judgements, especially of the Delhi High Court in *Mahindra & Mahindra Ltd. v. CCI & Anr.* (2019) SCC Online Del 8032. Given its *de-facto* constitution and functioning as a *quasi-judicial* tribunal, the DPB must comply with Article 323-B of the Constitution which allows for the creation of such tribunals through legislation, for one of the functions listed in clause (2) therein. However, the DPB is *ultra vires* of this provision as its core function (namely, data processing and data governance) is not listed in the said clause (2).

2. Necessary functions omitted: The DPB is currently framed as an adjudicatory body. However, given the nature of data protection risks and the need for a regulatory agency to ensure industry-wide implementation and awareness, the DPDP Bill must take into account certain important additional functions of the DPB.

Recommendation:

1. We recommend that clause 20(1) be amended and additional functions be added to ensure the DPB is performing the role of a full-fledged regulator and not limited to adjudication. Such expansion will ensure that it does not fall afoul of Article 323-B. Examples of such tribunals under other legislation include the Competition Commission of India (CCI) and the Securities and Exchange Board of India (SEBI). Both these regulators have a broader gamut of functions which *inter alia* include some adjudicatory role as well. The proposed DPB should have a similar scope of functions categorically listed in the legislation itself, to avoid confusion and a potential challenge to its constitutionality.

2. For example, Clause 11(2)(b) of the DPDP Bill requires significant data fiduciaries to appoint an independent data auditor and Clause 11(2)(c) requires significant data fiduciaries to conduct a data protection impact assessment and periodic audits. These compliances require in-depth technical knowledge. For such compliances to be implemented, the nodal agency (staffed with qualified members) is best suited for notifying qualifications, certifying data auditors, prescribing the manner in which data protection impact assessments may be carried out, and reviewing the reports from the data protection impact assessments and audits. Similarly, technology is ever-evolving, with newer challenges to data protection developing at a fast pace. The nodal agency (in this case, the DPB) must be empowered to undertake research, monitor technological developments and raise awareness regarding the obligations and responsibilities under the DPDP Bill. This will allow the DPB to coordinate with various departments across state governments and the central government, which routinely handle personal data, for capacity building and skill-training purposes.

3. Process to ensure compliance (Clause 21)

Context: This provision sets out the process through which the DPB may receive complaints from data principals, references from the state or central government, court directions or for violations of clause 16 (duties of a data principal), and take action under these complaints through inquiries and adjudication.

Issue:

1. Ambiguity about "techno-legal" methods: Under Clause 21(1), DPB should "as far as possible" function as a digital office and employ techno-legal measures as prescribed. This articulation is ambiguous and can potentially permit the use of predictive algorithms (commonly termed as artificial intelligence or AI) for adjudication of complaints. Such predictive justice algorithms have been found to be inaccurate, biassed, and lacking explainability and transparency. Furthermore, the Supreme Court's e-committee has categorically stated that any AI systems in the judiciary or judicial entities should be focused on improving administrative efficiency and not performing judicial functions.

2. Potential exclusion of certain data principals: Under Clause 21(1), the use of techno-legal applications at the DPB could potentially create an exclusionary effect, in the absence of adequate non-digital alternatives in place. he DPDP Bill establishes a right to grievance redressal under clause 14, which includes the right to file complaints against a data fiduciary if so desired [clause 14(2)]. Creating a completely digitised set up for dispute resolution could prove exclusionary for individuals who either lack access to the requisite digital infrastructure (like a smartphone, computing device, internet connectivity, etc.), or for those who are unfamiliar with the use of such technologies.

3. Lack on clarity: Under Clause 21(2), the provision is not clear on whether the DPB has suo-motu powers for taking cognizance of violations under Clause 16, or whether it can act against such breach of duty by data principals based on a reference made by a data fiduciary or any other entity.

4. Transparency: Under Clause 21(4), the DPB may determine that there are no sufficient grounds for proceeding with an inquiry, and may dispose of the complaint by putting its reasons in writing. If such reasons are not disclosed to the complainant, it may adversely impact the trust reposed by data principals in the DPB.

5. Timelines for DPB: Clause 21(8) states that inquiries shall be completed 'at the earliest'. This phrasing is unclear and not generally the manner in which inquiry timelines are established under law. Additionally, the DPB is restrained from blocking access to premises or taking into custody equipment or tools that may adversely affect the day-to-day functioning of the entity under investigation. Such a restraint may result in the DPB being unable to take into custody equipment even for the purposes of investigation and determining violations by the data fiduciary, even for the purposes of its function of enforcement of the DPDP Bill.

6. Only penalised if significant: Under Clause 21 (11), the DPB may determine that certain violations of the Bill by data fiduciaries are not significant, and may close inquiries without any penalties. Only if the violations are significant, the data fiduciaries may be punished for their actions through a financial penalty.

Recommendation:

1. We recommend that additional clarity be provided to this provision, or that this provision be redrafted to better reflect the reasoning behind the use of this phrase. Further, the use of any techno-legal methods should be in consultation with the Supreme Court e-committee, before being prescribed through subsequent rules. Predictive algorithms for adjudication of complaints should be categorically excluded from use under Clause 21(1).

2. Adequate alternative modes for raising complaints, as well as getting redressal should be made available. The digital mode of dispute resolution should be voluntary and not mandatory under subsequent rules.

3. In this provision, the DPB must be empowered to *suo motu* take cognizance of instances of violations of the provisions of the DPDP Bill, and initiate suitable inquiries under the Bill.

4. A transparency obligation that discloses these reasons to the complainant must be included within this provision.

5. Under clause 53(5) of the PDP Bill 2019, data fiduciaries, processors and their agents were required to produce data within their custody before the inquiry officer, who could then retain this data for up to six months. This provision allowed the inquiry officer to carry out his duties under the PDP Bill 2019. The current framework casts the DPB as a toothless entity restrained from even this basic power. We recommend that this provision be omitted in favour of introducing newer provisions that clarify the powers of the DPB in line with their enforcement-related duties under this Bill.

6. We strongly disagree with the reasoning behind this provision, and recommend that this provision be omitted from the DPDP Bill. Failure to clarify what constitutes a 'significant' violation of the provisions of the DPDP Bill allows for arbitrary decision-making by the DPB. Further, the rights of the data principal are substantially weakened if their violations are only punishable if they are deemed significant enough. Violations of obligations under the DPDP Bill must be punishable *per se*, with significant violations being punished through greater sanctions. However, the current framing of the law allows data fiduciaries violating the statute to evade their obligations and go scot-free if these violations are not 'significant'.

4. Voluntary Undertaking (Clause 24)

Context: The DPB may accept a voluntary undertaking to act or refrain from acting in a particular manner at any stage regarding compliance with the provisions of the Bill. Once the voluntary undertaking is accepted by the DPB, it shall act as a bar on proceedings under this Bill for those particular actions specified within the voluntary undertaking. Failure to act in accordance with the voluntary undertaking may result in the person being penalised.

Issue: The provision in its current iteration is extremely broad, and allows data fiduciaries to submit a voluntary undertaking at any stage. Such undertaking may also be submitted after the

data fiduciary has been found guilty of significantly breaching the provisions of the bill, to evade the financial penalty those violations carry. This provision allows too much leeway to data protection data fiduciaries breaching statutory duties, and undermines the accountability framework under this Bill.

Recommendation: We recommend that this provision be structured to incentivise data fiduciaries to not breach any of their duties under this Bill, as opposed to its current form which allows data fiduciaries to evade accountability for their actions up to the stage of levying financial penalty. This can be ensured by limiting the voluntary undertaking scheme to stages prior to issuance of notice for inquiry by the DPB under Clause 21. Additionally, voluntary undertakings issued by data fiduciaries must mandatorily include provisions of compensating data principal and rectifying the damage the voluntary undertaking pertains to violations of the rights of data principals.

5. Financial Penalty (Clause 25)

Context: This provision, read with Schedule 1, sets out the financial penalties prescribed for significant violations of this Bill's provisions. It also sets out certain additional factors that the DPB must take into account while determining the penalty.

Issue:

1. Penalty for re-identifying anonymised data: There is no penalty prescribed for re-identifying anonymised data. Since large amounts of personal data is anonymised and shared as non-personal data, the rest of this bill does not apply to such provisions. It has been established in several studies that anonymised data can be re-identified, which presents a huge risk to privacy.[16]

2. Compensation for data principals: The current framework does not provide relief to data principals as a result of any violation of the DPDP Bill by a data fiduciary or a data processor through monetary compensation.

Recommendation:

1. Personal data that has been anonymised must have its anonymity guaranteed to prevent privacy violations. This can be ensured by prescribing a higher penalty for any manner of re-identification of anonymised data. For reference, the DPDP Bill can include a provision similar to Clause 82 of the PDP Bill 2019.

2. We recommend including a separate provision that allows data principals to seek compensation from the data fiduciary or data processor. This compensation amount can be determined by the DPB taking into account the harms suffered by the data principal,

[16] Christine Porter 'De-Identified Data and Third Party Data Mining: The Risk of ReIdentification of Personal Information' (2008) 5 Shidler J.L. Com. & Tech. 3 <https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi? article=1075&context=wjlta>; Dalal Al-Azizy et al 'A Literature Survey and Classifications on Data De-anonymisation' (2015) International Conference on Risks and Security of Internet and Systems 36 <https://orbilu.uni.lu/bitstream/10993/37611/1/article-2576.pdf>; Arvind Narayanan and Vitaly Shmatikov 'Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)' (2008) <https://arxiv.org/pdf/cs/0610105.pdf>

the nature of the violation and other mitigating or aggravating factors. This compensation awarded to the data principal as monetary relief as compensation for the harms suffered must be distinct from the financial penalties levied on data fiduciaries or data processors for violating the provisions of the DPDP Bill 2019.