CUTS Comments on the draft Digital Personal Data Protection Bill, 2022

Authored by:

Neelanjana Sharma, Prince Gupta and Asheef Iqubbal

Senior Research Associates, Consumer Unity & Trust Society

CUTS International

CUTS Comments on the draft Digital Personal Data Protection Bill 2022

Background

Consumer Unity & Trust Society (CUTS) expresses its gratitude to the Ministry of Electronics and Information Technology (MeitY) for inviting comments and suggestions on the draft Digital Personal Data Protection Bill, 2022 (Bill, or DPDPB). Enacting a data protection law is critical to safeguarding the Right to Privacy of Indian citizens.

About CUTS

In its 39 years, CUTS has come a long way from being a grassroots consumer-centric organisation based in Jaipur to opening overseas Resource Centres in Africa,[1] Switzerland,[2] Vietnam,[3] and most recently in the United States of America.[4] It continues to remain an independent, nonpartisan, and non-profit economic policy think tank while opening various programme centres, namely: Centre for International Trade, Economics & Environment (CITEE);[5] Centre for Consumer Action, Research & Training (CART);[6] Centre for Human Development (CHD);[7] and Centre for Competition, Investment & Economic Regulation (CCIER).[8] It has been working towards enhancing the regulatory environment through evidence-based policy and governance-related interventions across various sectors and national boundaries. Further details about CUTS are available here.

Having conducted various studies in area of inclusive digital economy[9] on issues pertaining to data protection,[10] data localisation,[11] children's data protection,[12] and encryption,[13] CUTS has observed a few critical issues in the draft Bill. These have been discussed in subsequent sections, along with a few recommendations to address them.

We have made general as well as clause-by-clause comments on the DPDP Bill.

CUTS General Comments

CUTS appreciates the public consultation process undertaken by MeitY and submits its comments below to that end. Moving away from its previous version, the draft Bill skips mention of the fundamental Right to Privacy in its Preamble, which is a regressive step. Further, it narrows the scope of the law from data protection to digital personal data protection,

1 http://www.cuts-international.org/ARC/
2 http://www.cuts-geneva.org/
3 http://www.cuts-hrc.org/
4 http://www.cuts-wdc.org/
5 https://cuts-citee.org/
6 https://cuts-cart.org/
7 https://cuts-chd.org/
8 https://cuts-ccier.org/
9 https://cuts-ccier.org/digital-economy/
10 https://cuts-ccier.org/cdpp/
11 https://cuts-ccier.org/understanding-impact-of-data-localization-on-digital-trade/
12 https://cuts-ccier.org/highlighting-inclusive-and-practical-mechanisms-to-protect-childrens-data/
13 https://cuts-ccier.org/understanding-consumers-perspective-on-encryption/

excluding non-personal data, which is rather desirable. In doing so, the draft Bill takes away the categorisation of personal data, especially sensitive personal data, thereby painting all personal data with the same regulatory brush.

It is a welcome move that the classification of Significant Data Fiduciaries has evolved from only the number of registered users as in intermediary rules. The factors include the volume and sensitivity of personal data processed, risk of harm to the Data Principal, and risk to electoral democracy and public order, among others. While the move to allow the transfer of personal data outside India appears to be a step forward, the draft Bill provides significant unreasonable discretion to the Central Government to notify trusted countries for such transfer, without necessary principles or procedural safeguards. The draft Bill could have prescribed better regulation and rule-making processes, including notice and comment period, cost-benefit analysis, and transparent stakeholder consultations. These practices are the hallmark of maturing the regulatory ecosystem, and can also help in the appropriate exercise of executive discretion. To this end, CUTS recommends:

a. Use of Regulatory Impact Assessment (RIA) Mechanisms:

The DPDPB is a legislation that frames out the rights and duties of the citizens (Digital Nagriks) on the one hand and the obligations to use collected data lawfully of the Data Fiduciaries on the other hand. There is recognition that laws and rulemaking for the internet have to be around the basic foundational principles and expectations of our citizens of openness, safety & trust and accountability.[14]

To realise this goal, conducting a Regulatory Impact Assessment (RIA) through mechanisms like Cost-Benefit Analysis (CBA) before enacting the new law and the rules that will be prescribed at a later is necessary. Regulatory instruments have widespread impacts, and affect multiple stakeholder groups in different ways. Sub-optimal regulations have the potential to impose unintended cost of administration and compliance, leading to adverse outcomes, thereby reducing the likelihood of achievement of its objectives. It is therefore important to understand the impacts of any proposed regulation, to achieve favourable outcomes.

RIA systematically identifies and assesses regulatory proposals' direct and indirect impacts using consistent analytical methods. It involves a participatory approach via a public consultation to assess such impact, determine costs and benefits, and select the most appropriate regulatory proposal. It also helps put checks and balances on the government while exercising its exclusive privilege to do things necessary to protect the data of Indian citizens. It is, therefore, recommended that the government engages with organisations experienced in conducting RIA before finalising provisions of the new law. Conducting adequate stakeholder consultations would also be helpful in this regard.

b. Having Procedural Safeguards in Place:

DPDPB leaves the safeguards to imagination or to be prescribed at a later date. We recommend that procedural safeguards be installed in the Bill before it is released for public use. The safeguards would ensure accountability and transparency in the process of protection of digital personal data. Procedural safeguards would include equal opportunity to be heard, reasoned orders and signing off on rules and executive decisions by significantly higher officers or judicial officers. This can be ensured by way of approved policies, procedures, standards and

[14] Explanatory Note to Digital Personal Data Protection Bill, 2022, *available at* Explanatory Note- The Digital Personal Data Protection Bill, 2022

guidelines for operating platforms and businesses in India.

c. Substantive Safeguards should be Inbuilt into the Law:

To protect the individuals' Right to Privacy, substantive safeguards must be tailored into the fabric of the law itself. These safeguards would mean clarity in drafting terms and inclusion of principles of legality, necessity and proportionality within the processes of law. Enhancing transparency for digital nagriks that the law aims to protect should be an important facet of the law in its written form and its implementation.

d. Support Consumer Interest Groups:

As the latest law focuses on protecting digital personal data of digital nagriks, the Right of Grievance Redressal must be similarly protected. The model of grievance redressal incorporated in the law needs to be strengthened with exercises that raise awareness and the capacity of consumers to enforce their rights. Thus, CUTS recommends that the Bill also provides for creation of a "Data Protection Fund" and the provision should require the Board to support relevant stakeholders such as centre and state governments, Data Fiduciaries etc. to undertake user awareness generation and capacity building activities as part of their responsible business activities in India. For this purpose, groups that work in favour of consumer interest should be involved in the awareness and capacity building process. The Bill also provides for penalties on data fiduciaries, the funds collected through these provisions should be utilised in accordance to the doctrine of 'cy pres'. through this, the funds can be put to the 'next best use,' which may include awarding funds to public interest organisations for the purposes related in some way to the case.[15]

e. Ensure Competition and Level-playing Field through Rule-making Process:

The Bill in its present form has been formulated to keep it as brisk and avoid being overly prescriptive. To ensure this, the law has left rules to be prescribed later at 18 different places. We hope that when these rules are prescribed later, they will follow the principles of equality. Rules made later on should treat different entities differently in a manner that does not create any advantageous position favouring any entity. This would ensure competition in the dynamic digital economy landscape while favouring innovation through start-ups, and small and medium-sized enterprises.

f. Need for a Data Protection Regulator:

Various issues have plagued the sectors working in the digital economy. For instance, all interconnected networks end up with enmeshed data, which further ends up being shared with entities for different purposes such as debt recovery, credit offers, targeted advertising etc. Often consumers are harassed for information and further subscription. To protect the interest of consumers, there should be a data protection regulator that is responsible for overseeing the data protection approach, strategy, and its implementation. Further, making regulations for issues such as ways for Data Fiduciaries and Data Processors to determine the age of Data Principal and practices to be adhered to for ensuring data protection is necessary. Instead of the Central Government, a specialised regulator should perform such functions, because it is already overburdened with numerous tasks. Moreover, giving the Central Government regulatory and supervisory powers leads to a conflict of interest as it is a Data Fiduciary.

The regulator may also envision a co-regulatory mechanism wherein, the industry, civil society

[15] CUTS- CIRC Submission to Competition Law Review Committee, *available at* https://cuts-ccier.org/pdf/CUTS-CIRC_Submission_to_Competition_Law_Review_Committee.pdf

and all general public can suggest regulatory practices which can be mandated after performing a cost-benefit analysis and due public consultation in a transparent manner. Further, the regulator should set its annual agenda in consultation with stakeholders and ensure that it is able to achieve its stated goals, which will bring in a mechanism of accountability. The regulator should make use of technology to manage complaints. For instance, Regulatory Technology (RegTech) and Supervision Technology (SupTech) help simplify, streamline, and automate regulatory compliance processes and help reduce the risk of fines, penalties, and legal implications.[16] Recently, the Telecom Regulatory Authority of India (TRAI), incorporated use of Distributed Ledger Technology (DLT) to control Unsolicited Commercial Communication.[17]

Additionally, it is important to hold the regulator accountable for its action. For this purpose, the responsibility can be provided to the Parliamentary Standing Committee on Information Technology or Standing Committee on Subordinate Legislation. All proceedings conducted can be live streamed, for ensuring transparency. This will instil confidence in the Data Principals and the public about the regulator being an independent body.

[16] Sharma, Neelanjana, 'Impact of Unnecessary Compliances on Ease of Doing Digital Business', July 2022, *available at* Impact of Unnecessary Compliances on Ease of Doing Digital Business in India | Cuts CCIER

[17] Gupta, Pavan, 'Use of Distributed Ledger Technologies to control Unsolicited Commercial Communication', *available at* https://trai.gov.in/sites/default/files/DLT_UCC_28012022.pdf

CUTS' Clause-by-Clause Suggestions and Rationale:

Clause No.	Digital Personal Data Protection Bill 2022	Suggested Amendments	CUTS Comments and Rationale
		Preamble	
Preamble	The **purpose** of this Act is to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process personal data for lawful purposes, and for matters connected therewith or incidental thereto.	The purpose of this Act is to provide for the processing of digital personal data in a manner that **protects** the Right of individuals to protect their personal data. **The Act also recognises** the need to process personal data for lawful purposes **with individual's consent.** **The Act strives to protect the fundamental Right to Privacy and the personal data of an individual as an essential facet of informational privacy.** **The Act will uphold the principles of Right to Privacy in processing of digital personal data. For this, the Act will uphold the principles of data minimisation, purpose limitation, and storage limitation.**	Preamble of any law lays down the main objectives which it seeks to achieve. *The preamble of the statute is a good means to find out the meaning of the statute and as it were a key to open the understanding thereof.*[18] The previous draft of the Bill, the Data Protection Bill 2021 (DPB '21), released in the Joint Parliamentary Committee (JPC) Report in 2021 had a lengthier preamble which included a more elaborate purpose and objective of the law. For instance, the 2022 draft skips the mention of Right to Privacy acknowledged to be part of Article 21 in 2017 Puttaswamy Judgement.[19] The mention of Right to Privacy in the Preamble would mean that achieving said Right shall become the founding principle for the law. The explicit mention of Right to Privacy would lead to the holistic interpretation of the law in line with the principles of Right to Privacy. CUTS understands that data protection is important in

[18] Sir Edward Coke (1 Inst. 79a cited at page 186 of Craies on Statute Law, Fifth Edition

[19] Draft DPDP Skips 'Right to Privacy' In Preamble, Govt Gets Unrestrained Powers: CUTS

			today's world to empower the nation's digital nagriks. Thus, the need of the state to leverage collective data should not take over the individual's Right to Privacy. CUTS recommends that the preamble retains the mention of the Right to Privacy being a fundamental right from the 2021 draft Bill. Further, the preamble only recognises the Right of individuals to protect their personal data, and it should strive to protect the same. The Bill should not favour a trade-off between protecting and processing personal data. Thus, data protection should continue to happen even during the processing of data, which should be subject to the consent of the individuals. The explanatory note accompanying the DPDPB lays down five principles, which should be reflected in the preamble to give them legal enforceability.
CHAPTER 1: PRELIMINARY			
1. Short Title, Extent and Commencement			
(1)	This Act may be called the Digital Personal Data Protection Act, 2022.	-	The Act has narrowed the scope of the law by removing non-personal data (NPD) and limiting the law to digital personal data. CUTS, in its research-based advocacy study earlier this year, had called for the exclusion of NPD from the applicability ambit of the draft DPB'21.[20] CUTS welcomes the exclusion of NPD from the 2022 draft Bill.

[20] Narayan, Sidharth and Sinha, Visushi, 'Non-Personal Data 2.0: Mapping the way forward for optimal regulation of Non-Personal Data' July 2022, *available at* https://cuts-ccier.org/pdf/report-non-personal-data-2-0.pdf

2. Definitions			
2. (3)	"child" means an individual who has not completed eighteen years of age;	**"Child" would have the following classifications under its meaning:** **Individual aged 13 and under would be referred to as "child,"** **Individuals above the age of 13 and under the age of 18 would be referred to as "teenagers" and treated as adults in matters of consent and protected as children in matters of abuse.**	The definitions provided in the recent draft is the same as the one used in the previous draft of the Bill. Indian law uses the same definition across criminal and civil laws. However, with the rising usage of the internet amongst youth and vast cultural differences, this approach might not be sustainable in the long run. The draft Bill has taken a 'one-size fits all' approach and equated the maturity level of all individuals aged below 18 years of age. Notably, as has been acknowledged by the JPC report, other jurisdictions like the US and the UK have adopted lower age thresholds.[21] CUTS has undertaken a large evidence led-study[22] which found that children have already been operating internet-enabled devices from the age of 14 years without parental guidance. The study also finds that over 75 percent of parents believe that their child knows more than them about practices to adopt for a safe online experience. They can provide consent to the terms & conditions of service providers, a claim seconded by around 73 percent of young users.[23] Further, the fluidity of young people's attitudes and perspectives as they eagerly embrace growing social media, gaming platforms and mobile apps, calls for a

[21] Gupta, Prince, 'Children's Data Protection' January 2022, *available at* https://cuts-ccier.org/pdf/bp-childrens-data-protection.pdf
[22] See https://cuts-ccier.org/highlighting-inclusive-and-practical-mechanisms-to-protect-childrens-data/
[23] Gupta, Prince, 'Children's Data Protection' January 2022, *available at* https://cuts-ccier.org/pdf/bp-childrens-data-protection.pdf

			principle-based regulation. Building upon the 'precautionary principle' used for ensuring foods, drugs and other products do not cause any harm, a similar approach should be undertaken with respect to children's data.[24]
2. (13)	"personal data" means any data about an individual who is identifiable by or in relation to such data;	"personal data" means any data about an individual **who is directly or indirectly identifiable, having regard to any physical, psychological, mental, cultural or social characteristic, trait, attribute or any other feature of the identity of such natural person whether online, offline, or any combination of such features with any other information and shall include any inference drawn from such data.**	Moving further away from the definitions of personal data in the previous versions of the Bill, this version has completely done away with categorising data into sensitive personal data (SPD) and critical personal data (CPD). In its previous submissions, CUTS noted that the definition of personal data is contingent upon the 'identifiability' of the person through such data. But, this criterion of 'identifiability' may differ depending upon the person's social, economic, cultural profile and intimacy towards relevant data.[25] Anonymisation of data to limit the potential identifiability of the information that might not directly identify individuals will not be enough. Individuals may become identifiable when such information is viewed with other pieces of information that one has access to or knows. This is known as 'jigsaw' identification. To prevent this, identifiability needs to be looked at from the viewer's perspective.[26]

[24] Montgomery, Kathryn C., et. al, 'Data governance for young people in the commercialised digital environment', Issue brief no. 3, August 2020, Good Governance of Children's Data project, Office of Global Insight and Policy, UNICEF, *available at:* https://www.unicef.org/globalinsight/media/1081/file/UNICEF-Global-Insight-data-governance-commercialization-issue-brief-2020.pdf

[25] Heda, Shubhangi, 'Key Definitions in the Personal Data Protection Bill 2019, *available at* https://cuts-ccier.org/pdf/policy-brief-key-definitions-in-the-personal-data-protection-bill-2019.pdf

[26] GDPR Identifiability, anonymisation, guidance note 5, *available at* https://www.ukri.org/wp-content/uploads/2021/11/MRC-291121-GDPR-Identifiability-Anonymisation-Pseudonymisation.pdf

			This is also informed by the CUTS user perception survey on privacy and data protection, which observed that different users (based on gender, age, years of using the internet etc.) perceive different information differently. For instance, female users are more uncomfortable in sharing their email ids, compared to male counterparts or more adults are uncomfortable in sharing their personal photos compared to younger people.[27] Hence, it is important to consider user perspectives while determining 'identifiability' which can be defined by identifiers of perception and perceived sense of intimacy and necessity. Similar identifiers are also provided in the European Union's General Data Protection Regulation (GDPR).[28] Personal data and its meaning should reflect the users' perceived risk of misuse or potential harm along with providing a guiding principle for categorisation of such data. In this regard, being informed by Japan's Act of the Protection of Personal Information (APPI).[29]
2. (14)	"Personal data breach" means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data,	"Personal data breach" means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data that compromises the	The latest draft has modified the definition of personal data breach from the previous versions. Previous versions maintained that personal data breach meant any unauthorised or accidental disclosure, acquisition etc. The latest version adds processing of the data to the

[27] Amol Kulkarni and Swati Punia, "Users' Perspectives On Privacy And Data Protection" *available at* https://cuts-ccier.org/pdf/survey_analysis-dataprivacy.pdf

[28] GDPR, Article 4(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[29] Japan's Act of the Protection of Personal Information (APPI), https://www.ppc.go.jp/en/

	that compromises the confidentiality, integrity or availability of personal data.	confidentiality, integrity or availability of personal data. **It shall also include authorised processing of data which does not adhere to the principles of legality, necessity and proportionality.**	definition which is a welcome step. However, the definition of personal data breach can include any authorised processing done beyond the principles of legality, necessity and proportionality. It is likely that these principles are added to the clauses relating to processing of personal data. However, to reinforce the primary focus on digital personal data protection, it is desired that the principle of Right to Privacy be reflected in all clauses. It would ensure that in processing of data no adverse interpretations are made which are violative of the fundamental Right to Privacy protected under Article 21 of the Indian Constitution.
2.(18)	"public interest" means in the interest of any of the following: a. sovereignty and integrity of India; b. security of the State; c. friendly relations with foreign States; d. maintenance of public order; e. preventing incitement to the commission of any cognizable offence relating to the preceding sub-clauses; and f. Preventing dissemination of false statements of fact.	"public interest" **shall** mean in the interest of any of the following, **given that these are under substantial risk**: a. sovereignty and integrity of India; b. security of the State; c. friendly relations with foreign States; d. maintenance of public order; **e. xx** **f. xx**	The definition of public interest did not find its place in the previous versions of the Bill. It is appreciated that the latest draft Bill has tried to define the same. However, this interpretation of the term is broad and vague and would include several scenarios which might not be in the general public's interest. Further, sub-clauses (e) and (f) focus on invoking public interest with the intention of preventing certain actions. These clauses can be used for abuse of power and weigh heavily against freedoms provided under Article 19. For instance, the pre-emptive prohibition of peaceful protests and publications can be one of the potential misuses. The law should look towards public interest as something not generic but special in nature which is invoked after procedural safeguards for prevention of harm have already been exhausted.

			The Data Protection Act 2018 of the United Kingdom in correlation to clause 6(1) of GDPR in Schedule 8 elaborating upon the conditions for sensitive processing, asks for the same to be done specifically for *substantial public interest*.[30] Substantial public interest means the public interest needs to be real and of substance. Given the inherent risks of personal data, it is not enough to make a vague or generic public interest argument, the processing of data needs to have concrete wider-ranging benefits supported by specific arguments.[31] CUTS recommends that the definition of public interest be amended. The conditions in sub-clauses a, b, c and d are too broad and should be broken down into their sub-components. Further, public interest as an exception should be invoked only when these components are under substantial risk.
3. Interpretation			
3. (1)	unless the context otherwise requires, a reference to "provisions of this Act" shall be read as including a reference to Rules made under this Act.	unless the context otherwise requires, a reference to "provisions of this Act" shall be read as including a reference to Rules made under this Act. **New subsection to be inserted as subsections 3 (4), (5), (6), (7) and (8):**	There are no corresponding clauses for this clause in the previous versions of the Bill. It is a welcome step as the Interpretation clause becomes the window into the mind of the lawmakers and allows for clear objectives to be undertaken in the further rule-making process. It might be useful for the interpretation clause to include the principles of legality, necessity and proportionality for

[30] Identifiability, anonymisation and pseudonymisation, GDPR Guidance note 5, *available at* https://www.legislation.gov.uk/ukpga/2018/12/schedule/8/enacted
[31] Through the UK Information Commissioner Website: See What are the substantial public interest conditions? | ICO.

		(2) The rule making authority must publish a draft of a proposed rules, accompanied with a statement setting out, – **(a) the objectives of the proposed rules;** **(b) the problem that the proposed rules seek to address;** **(c) how solving this problem is consistent with the objectives under this Act;** **(d) the manner in which the proposed rules will address this problem;** **(e) the manner in which the proposed rules comply with the provision of this Act under which the rules are made;** **(f) an analysis of costs and an analysis of benefits of the proposed rules;** **(g) the process by which any person may make a representation in relation to the proposed rules;**	the rules made under this act. Further, the Bill must mandate adopting scientific regulatory decision-making processes, to frame optimal regulations, wherein the costs of regulations do not outweigh their intended benefits. The rule-making authority must undertake time-bound public consultation and should also review the justification of regulations from time to time. The inclusion of sunset clauses for regulations has been recommended in this regard. Inspiration may be taken from the Indian Financial Code.[32] A similar approach has been adopted by the IBBI where it has developed a transparent and consultative process to regulation making.[33] In 2013, the Financial Stability and Development Council (FSDC) recommended a similar rule-making process.[34] Similarly, the 'sunset clause' has also been adopted in the 2021, Drone Rules.[35] Thus, new sub-sections should be added which have been provided in the suggested changes.

[32] CUTS Submission to the Joint Committee on The Personal Data Protection Bill, 2019, *available at* https://cuts-ccier.org/pdf/submission-pdpb-2019.pdf
[33] Kumar, Saji, K.R, 'Walking the Regulatory Tightrope' *available at* https://ibbi.gov.in/uploads/resources/21c2c7926595cbf2f641ad42392eeb4d.pdf
[34] Financial Stability and Development Council, Government of India, ed., FSDC Meeting dated October 24, 2013, ANNEXURE B (Implementation of Non-Legislative Recommendations of FSLRC), Oct. 24, 2013. Also, See Handbook on adoption of governance enhancing and non-legislative elements of the draft Indian Financial Code, pg. 39, *available at* https://dea.gov.in/sites/default/files/Handbook_GovEnhanc_fslrc_2.pdf
[35] The Drone Rules, 2021, *available at* https://egazette.nic.in/WriteReadData/2021/229221.pdf

		For the purpose of this Act, when carrying out an analysis of costs and benefits, collectively termed cost-benefit analysis, the rule making authority must consider probable costs that will be borne by and the probable benefits that will accrue to persons affected by the rules, including but not limited to, Data Principals, Data Fiduciaries, Data Processors, and the rule making authority. **Use of best available data, and wherever not available, reasonable estimates, to carry out the analysis; and the most appropriate scientific method available to carry out the analysis should be made.** **(3) The rule making authority must:** **(a) give a time of not less than thirty days to enable any person to make a representation in relation to the proposed rules and consider all representations made to it within that time.** **(b) publish all the representations received by it along with a general account of the response of the rule making authority to the**	

		representations. **(4) If the rules differ substantially from the proposed rules, the rule making authority must publish the details and reasons for such difference; and an analysis of costs and an analysis of benefits, of the differing provisions.** **(5) Every rule made, should be reviewed within three years from the date on which that rule is notified. The review must comprise an analysis of:** **(a) costs and an analysis of benefits of the rules;** **(b) all interpretations of the rules made by relevant quasi-judicial and judicial authorities; and** **(c) the applicability of the rules to any change in circumstances since those rules were issued.** **(6) The report prepared by the rule making authority of such review(s) should be made public.**	
4. Application of the Act			
4. (1)	The provisions of this Act shall	The provisions of this Act shall apply	The sub-clause refers to the types of data that the Bill

	apply to the processing of digital personal data within the territory of India where: a. such personal data is collected from Data Principals online; and b. such personal data collected offline, is digitised	to the processing of digital personal data within the territory of India by **Data Processor, both public and private,** where **such personal data is collected, online or offline which is digitised, by Data Fiduciary, both public and private.**	refers to, which include data collected from Data Principals online and offline which is digitised later. This also provides for the inter-territorial application of the law and the processing of data done within the territories of India. The provision separates two types of personal data using the conjunction 'and' which legally means that the two are not mutually exclusive. However, experts have opined that the intent of the Bill seems inclined towards usage of 'or' where the law would apply to either of these situations.[36] CUTS recommends that clarity be brought forth in the regulation in the form of identifying the collector of data expressly in the provisions.
4. (2)	The provisions of this Act shall also apply to processing of digital personal data outside the territory of India, if such processing is in connection with any profiling of, or activity of offering goods or services to Data Principals within the territory of India. For the purpose of this	The provisions of this Act shall also apply to processing of digital personal data outside the territory of India, if such processing is in connection with any **automated decision making or** profiling of, or activity of offering goods or services to Data Principals within the territory of India. For the purpose of this subsection, "profiling" means any form of	This provision allows the Bill to have extraterritorial applications for processing outside the territory of India. For the purposes of the section, the definition used for profiling is too broad and indirect. For instance, the GDPR guidelines under Article 22[37] provides for definition of profiling which includes automated processing expressly. Article 4(4) of UK GDPR states that aspects of profiling can concern a person's performance at work, economic situation, health, personal preferences, interests, reliability,

[36] Rajesh, Varsha, et.al., 'Digital Personal Data Protection Bill, 2022: Analysis and Potential Impact on Businesses' 24 November 2022, Nishith Desai Associates, *available at* Nishith Desai Associates Digital Personal Data Protection Bill, 2022: Analysis and Potential Impact on Businesses

[37] Automated individual decision-making, including, profiling, *available at* https://gdpr-info.eu/art-22-gdpr/

	subsection, "profiling" means any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a Data Principal.	processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a Data Principal such **as economic situation, personal preferences, interests, reliability, location or movements etc.**	behaviour, location or movements.[38] It is one of the ways of circumventing the rights of Data Principals and their agency regarding their own data. Examples are an online decision to award a loan, approve a credit card etc. CUTS recommends that the applicability of data protection law be extended to automated-decision making and definition of profiling be extended to include the examples of profiling.
CHAPTER 2: OBLIGATIONS OF DATA FIDUCIARY			
5. Grounds for processing digital personal data			
5.	A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and Rules made thereunder, for a lawful purpose for which the Data Principal has given or is deemed to have given her consent in accordance with the provisions of this Act. For the purpose of this Act, "lawful purpose" means any purpose which is not expressly forbidden by law.	A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and Rules made thereunder, for a lawful purpose for which the Data Principal has given or is deemed to have given her consent in accordance with the provisions of this Act. For the purpose of this Act, "lawful purpose" means **any clear, concise and specific** purpose which is not expressly **and impliedly** forbidden by law.	The provision corresponds to Personal Data Protection Bill 2019's (PDPB'19) clauses 4 and 5 and provides for purpose limitation and grounds for processing of personal data. The provision is a welcome addition as it places importance on the consent of the Data Principal. However, it no longer requires personal data processing to be limited strictly to the purpose for which it was collected. This is known as the 'purpose limitation' principle, a key pillar of all data protection legislations around the world. The current version of the Bill allows personal data processing for any lawful purpose not expressly forbidden by law.

[38] Rights related to automated decision making including profiling, *available at* Rights related to automated decision making including profiling | ICO

			CUTS' user perception survey found that most consumers expected that the Data Fiduciaries should use the data only for the purpose of collection. The findings also reiterated that a few of the most flagged risks by consumers were the fear of additional data collection, by data fiduciaries or data being used for undisclosed purposes, along with misuse of data for unauthorised purposes.[39] Also, the definition of 'lawful purpose' is myopic and does not consider the potential misuse of '*expressly forbidden by law*'. Where laws should bring clarity, this definition creates a grey area that will lead to the need for judicial interpretation later.[40] To avoid the gaps left by expressly forbidden by law, the rule of implied prohibition should be adopted. *This principle of statutory interpretation according to which, when a law or a statute directs that a thing is to be done in a certain way, then even if there are no negative connotations or words attached to it, that thing shall not be done in any other way. The court shall attach a construction which effectuates the legislative intent and purpose.*[41] This should be clearly reflected in the law.

[39] Mehta, Udai, 'CUTS comments on draft Personal Data Protection Bill 2018', *available at* https://www.cuts-ccier.org/pdf/Advocacy-CUTS_Comments_on_the_draft_Personal_Data_Protection_Bill2018.pdf

[40] Singh, Vikram Jeet and Daga, Prashant, 'Third Time's The Charm? Unpacking The Draft Digital Personal Data Protection Bill, 2022', 1 December 2022, *available at* https://www.mondaq.com/india/privacy-protection/1256536/third-time39s-the-charm-unpacking-the-draft-digital-personal-data-protection-bill-2022

[41] M/s Apex Laboratories Pvt. Ltd. v. Deputy Commissioner of Income Tax, Large Tax Payer Unit - II, 25 February 2022, *available at* https://www.livelaw.in/pdf_upload/332592019215013361 8judgement22-feb-2022-1-410313.pdf

			CUTS recommends that the grounds of processing data be based on *consent, purpose limitation and lawful purpose*. For this, the definition of lawful purpose should be amended and provision be expanded in favour of processing of data collected for lawful purposes. For this, inclusion of words emphasising the requirement of specificity, clarity, fairness and reasonableness for collection and processing of personal data should be done.
6. Notice			
6. (1)	On or before requesting a Data Principal for her consent, a Data Fiduciary shall give to the Data Principal an itemised notice in clear and plain language containing a description of personal data sought to be collected by the Data Fiduciary and the purpose of processing of such personal data.	On or before requesting a Data Principal for her consent, a Data Fiduciary shall give to the Data Principal an itemised notice in clear**, concise** and plain language **which is easily comprehensible to a reasonable person** containing a description of personal data sought to be collected by the Data Fiduciary and the purpose of processing of such personal data. **For the purpose of this section: -** **(a) "notice" shall mean privacy labels on the lines of nutrition labels or energy labels, which are a**	The notice provision under the 2022 draft Bill merely states that an itemised notice in clear and plain language should be provided, but does not list out the information that is required to be provided in the notice, which is provided in detail under the PDPB'19. Also, the provisions though intended to provide useful user protection to Data Principals, however the efficacy of the provisions remains doubtful. The provisions make a biased assumption of users being cognizant and capacitated of reading and understanding notices of data collection, and providing informed consent for the processing of their data. CUTS' user perception pointed out that most people don't read privacy policies (notices), mostly due to their exhaustive length.[42] Therefore, we suggest that all notices

[42] Kulkarni, Amol and Swati Punia, "Users" Perspectives on Privacy and Data Protection" *available at* https://cuts-ccier.org/cdpp/

		multilingual/ info-graphic communication tool to provide clear, transparent and multi-layered privacy information to Data Principals. Notice can be a separate document, or an electronic form, or a part of the same document in or through which personal data is sought to be collected, or in such other form as may be prescribed. **(b) "itemised" means presented as a list of individual items. Out of these the Most Important Terms and Conditions (MITC) should be prominently displayed and requested for acknowledgement.**	provided be "clear, concise and easily comprehensible to a reasonable person." For this purpose, CUTS advocates the use of 'privacy labels' similar to 'nutrition labels' and 'energy labels'[43] by operators and service providers. These label's efficacy can be tested by use of a regulatory sandbox. These have been accepted as means of ensuring innovation within contained means leading to evidence-led regulatory environment.[44] Further, the regulator must prescribe that Most Important Terms and Conditions (MITC) should be prominently displayed and requested for acknowledgement. This has been required in the RBI's digital lending guidelines.[45]
6. (2)	Where a Data Principal has given her consent to the processing of her personal data before the commencement of this Act, the Data Fiduciary must give to the Data Principal an itemised notice in clear and plain language containing a	Where a Data Principal has given her consent to the processing of her personal data before the commencement of this Act, the Data Fiduciary must give to the Data Principal an itemised notice in clear**, concise** and plain language **which is easily comprehensible to a**	The provision reads well and it is laudable that consent given for processing before the commencement of the Act also would require an itemised notice. However, not setting a time limit on Data Fiduciary for providing said notice other than when reasonably practicable is giving Data Fiduciary a loophole to circumvent the notice process altogether.

[43] See CUTS' Consumer Broadband Labels' Brochure https://cuts-ccier.org/pdf/Brochure-Information_Labels_for_Consumers.pdf

[44] RBI Enabling Framework for Regulatory Sandbox, *available at* Department of Banking Regulation Banking Policy Division Enabling Framework for Regulatory Sandbox Contents 1. Background 02 2.

[45] Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps, 18 November 2021, *available at* https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1189

	description of personal data of the Data Principal collected by the Data Fiduciary and the purpose for which such personal data has been processed, as soon as it is reasonably practicable. For the purpose of this section: - (a) "notice" can be a separate document, or an electronic form, or a part of the same document in or through which personal data is sought to be collected, or in such other form as may be prescribed. (b) "itemised" means presented as a list of individual items.	**reasonable person** containing a description of personal data of the Data Principal collected by the Data Fiduciary and the purpose for which such personal data has been processed, as soon as it is reasonably practicable, **no later than three months from the commencement of the act, as may be prescribed**.	Therefore, the addition of a reasonable time frame within which notice must be provided must be added by the regulator. Explanation of "notice" and "itemised" has been shifted to clause 6(1).
6. (3)	The Data Fiduciary shall give the Data Principal the option to access the information referred to in sub-sections (1) and (2) in English or any language specified in the Eighth Schedule to the Constitution of India.	The Data Fiduciary shall give the Data Principal the option to access the information referred to in sub-sections (1) and (2) in English or any language specified in the Eighth Schedule to the Constitution of India. **Such an option should be provided for in the notice in subsections (1) and (2) in a manner which is clear, concise and**	The draft Bill has specified that "languages specified in the Eighth Schedule of the Indian Constitution" can be used to provide said notice. This is a welcome step as it takes into account the vast regional and cultural diversity of India. The clause, however, has removed the requirement for the notice to be "clear, concise and easily comprehensible to a reasonable person" as was stated in the 2019 Bill.

		easily comprehensible to a reasonable person.	Service providers should not be allowed to use notices as a means to shrug away from their liability of data collection disclosure. On the contrary, the essence behind them should be to inform users about service providers' data processing practices and enable them to compare policies while making their decision.[46]
8. Deemed Consent			
8. (1)	A Data Principal is deemed to have given consent to the processing of her personal data if such processing is necessary: in a situation where the Data Principal voluntarily provides her personal data to the Data Fiduciary and it is reasonably expected that she would provide such personal data;	A Data Principal is deemed to have given consent to the processing of her personal data if such processing is necessary: in a situation where the Data Principal voluntarily provides her personal data to the Data Fiduciary and it is reasonably expected that she would provide such personal data **for a specified purpose and the Data Fiduciary will not process the data or store it beyond what is necessary for fulfilling said purpose**;	In situations where Data Principals voluntarily provide their personal data to a Data Fiduciary which is reasonable for them to provide, it would be deemed that the consent was provided for processing if such processing is necessary. The illustration of this section provides that a person might share their name and contact details with a restaurant for reserving a table. It would be deemed that they have provided the consent for the purpose of collection of such details. This might result in collection of data for unspecified periods of time and also as 'A' consented for the collection of personal data for the purpose of reserving, if the restaurant ends up processing that data beyond the reservation for reasons such as for informing them about offers, special occasion menus etc.

[46] Heda, Shubhangi, 'Notice and Consent Framework of the PDPB, Way Forward', *available at* https://cuts-ccier.org/pdf/policy-brief-notice-and-consent-framework-of-the-PDPB.pdf

			Though this might seem to be trivial. However, personal details such as contact details when shared trivially often end up becoming data stored and shared with multiple entities without the user's knowledge. This results in spam and promo messages, which has become a growing menace. Users' in a recent survey revealed that they receive unwanted and unsolicited messages over texts and WhatsApp which people feel should be addressed by telecom regulator,[47] Department of Telecommunications (DOT) and telecom companies working together.[48] It can be said that people in general when sharing their data do not understand its consequences.[49] In usual notice and consent frameworks, consent has been identified as broken,[50] therefore one can safely assume that deemed consent, not unlike normal consent, attracts unwanted attention from suspect entities. The details of several individuals may be enmeshed in any piece of content that is shared on a network, whether in the form of correspondence, aggregated information, photos, audio clippings or videos. Thus, an individual's or entity's voluntary sharing of such co-owned details might result in privacy intrusions and negative consequences for others in their network who never explicitly agreed to the

[47] Telecom Regulatory Authority of India (TRAI).
[48] Spam, promo messages: How menace is growing as users look for remedy - India Today
[49] Narayan, Vinay, 'DPDP Bill 2022: 'Deemed' Consent, To Users' Detriment', 12 December 2022, *available at* https://www.medianama.com/2022/12/223-dpdp-bill-2022-deemed-consent-to-users-detriment-views/
[50] Sinha, Amber and Mason, Scott, 'A Critique of Consent in Information Privacy', 11 January 2016, *available at* https://cis-india.org/internet-governance/blog/a-critique-of-consent-in-information-privacy

			sharing of that content.[51] Therefore, safeguards should be incorporated in the provision with time and purpose limitations to protect the interests of digital nagriks.
8. (8)	in public interest, including for: a. prevention and detection of fraud; b. mergers, acquisitions, any other similar combinations or corporate restructuring transactions in accordance with the provisions of applicable laws; c. network and information security; d. credit scoring; e. operation of search engines for processing of publicly available personal data; f. processing of publicly available personal data; and g. recovery of debt;	in public interest, for purposes that are including for: a. **Detection of fraud;** **b. xx** c. network and information security; **d. xx** e. operation of search engines for processing of publicly available personal data; f. processing of publicly available personal data; and **g. xx** **Explanation: publicly available data shall mean any data that Data Principal has consented to be made available publicly for the same purpose for which it is being processed.**	For the purpose of 'public interest' please see the suggestions made for clause 2(18) and amend the same accordingly. For sub-clause (a), prevention and detection of fraud: deemed consent and processing of data for prevention of fraud should be based upon substantial safeguards where consent is expressed and approval to process data for this purpose should be from higher authorities through reasoned orders and only if no other remedies are possible. For sub-clause (b), mergers and acquisitions etc. in no way can be termed as public interest. This should be omitted. In case it is retained, an explanation for the same should be released in public domain. For sub-clause (d) and (g), the inclusion of credit score and recovery of debt within the meaning of public interest might lead to unintended consequences. Operationalisation of digital financial services (DFS) heavily relies on a mix of personal data provided by consumers, and data collected and curated from multiple sources such as social media by the fintech platforms. This data of combined origin and ownership is further

[51] Carminati, B., & Ferrari, E. (2011, October). Collaborative access control in on-line social networks. In the 7th International Conference on Collaborative Computing: Networking, Applications and Work-sharing (CollaborateCom) (pp. 231-240). IEEE.

			shared by the platform with third parties for insurance, collection etc. this gives rise to a multi-party privacy (MPP) issue.[52] The enmeshed data ends up being shared with entities for debt recovery. In the name of debt recovery, consumers are harassed, faced with extortion, and some have committed suicide.[53] Therefore, to ensure financial well-being of the citizens and protect their Right to Privacy, credit scoring and recovery of debt must be removed from the deemed consent clause. For sub-clauses (e) and (f), processing of publicly available personal data is too broad and can subsume within its meaning illegal activities and illicit behaviour. Once personal data is publicly available for reuse, it will be increasingly difficult, if not impossible, to have any form of control over the nature of potential use. We must look at the underlying approach in both GDPR (no explicit consent needed for publicly available data) and in Canada's Personal Information and Electronic Documents Act (PIPEDA)[54] (express consent required for processing of publicly available data). The approach is that such processing should, to the greatest degree possible, be in line with the original purpose for which consent was initially obtained.[55]

[52] My Data or Yours, CUTS CCIER, See https://cuts-ccier.org/my-data-or-yours/
[53] A dark underbelly: Digital loans, real-world extortion | Deccan Herald
[54] Canada PIPEDA, *available at* The Personal Information Protection and Electronic Documents Act (PIPEDA) - Office of the Privacy Commissioner of Canada
[55] Udeozor, Benjamin I, 'Publicly available data: Privacy Considerations under GDPR and PIPEDA', 9 May 2021, *available at* https://www.linkedin.com/pulse/publicly-available-data-privacy-considerations-under-gdpr-udeozor/

			Therefore, publicly available data should have been uploaded with the consent of the Data Principal. Thus, an explanation must be added to the sub-clause for the meaning of publicly available data.
9. General obligations of Data Fiduciary			
9. (4)	Every Data Fiduciary and Data Processor shall protect personal data in its possession or under its control by taking reasonable security safeguards to prevent personal data breach.	Every Data Fiduciary and Data Processor shall protect personal data in its possession or under its control by taking reasonable security safeguards to prevent personal data breach. **Every Data Fiduciary and Data Processors strictly adhere to the principles of purpose limitation, data minimisation and collect limited data as is required for providing a service.**	Collection of data should not be misused by Data Fiduciaries by inducing Data Principals to share more data than required to provide the service. For example, when a user updates about their lunch, social media starts sending them pop-ups asking for the name of the place, restaurant, and with whom the user has visited which seems unnecessary and excessive information for the completion of the update. Platforms usually have been engaged in the practice of obtaining excessive information in the name of the completion of data. This should be taken into account by limiting the collection of personal information by Data Fiduciaries to what is directly relevant and necessary to accomplish a specified purpose and not to induce Data Principal to provide extra information.
9. (8)	Every Data Fiduciary shall have in place a procedure and effective mechanism to redress the grievances of Data Principals.	Every Data Fiduciary shall have in place a procedure and effective mechanism to redress the grievances of Data Principals **in a speedy and efficient manner**.	The clause has removed the words "efficiently and in a speedy manner". One of the core principles of effective grievance redressal is that it reaches the consumers efficiently and speedily. Further, to increase the effectiveness of grievance redressal mechanisms used by the Data Fiduciary,

			alternate dispute resolution mechanisms for grievance redress options should be explored. This could be done through setting up Consumer Service Cells on the lines of CUTS' initiative of Grahak Sahayata Kendra[56], which could act as a mediator or conciliator in resolving the complaints. At the same time, consumers should be provided with an easily accessible mechanism to lodge complaints and be updated about the same through toll free numbers, online portals, emails or in person.
9. (10)	**Insertion of New Clause**	**Every Data Fiduciary shall explicitly inform Data Principals about risks and consent requirements regarding voluntarily sharing their and other persons' data.**	CUTS study[57] has shown that most users do not read privacy policies and may be unaware of the risks involved with data sharing. Accordingly, users should be informed explicitly about risks and consent requirements regarding the voluntary sharing of their and other persons' data.
9. (11)	**Insertion of New Clause**	**Data Fiduciary shall periodically release a summary of the following to the data principal:** **(a) the confirmation whether the Data Fiduciary is processing or has processed personal data of the Data Principal;** **(b) personal data of the Data Principal being processed or that has been processed by the Data Fiduciary and the processing activities undertaken by the Data**	It is essential that data fiduciaries should participate in empowering data principals and take upon the positive obligation of providing data principal with the details regarding collection, processing and sharing of their information with the entity other than the original collector of data. Similar practices are observed by Mutual funds for investors, which can be relied upon.

[56] Consumer Care Centre (Grahak Sahayata Kendra) | CUTS Centre for Consumer Action, Research & Training (CART), *available at:* https://cuts-cart.org/consumer-care-centre-grahak-sahayta-kendra/

[57] 'Users' Perspectives On Privacy And Data Protection' Available At Https://Cuts-Ccier.Org/Pdf/Survey_analysis-Dataprivacy.Pdf

		Fiduciary with respect to the personal data of the Data Principal; **(c) the disclosure of personal data being shared with entities other than the data collecting data fiduciary.**	
10. Additional obligations in relation to processing of personal data of children			
10. (1)	The Data Fiduciary shall, before processing any personal data of a child, obtain verifiable parental consent in such manner as may be prescribed. For the purpose of this section, "parental consent" includes the consent of lawful guardian, where applicable.	The Data Fiduciary shall, before processing any personal data of a 'child' **aged 13 and under**, obtain verifiable parental consent in such manner as may be prescribed. For the purpose of this section, "parental consent" includes the consent of a lawful guardian, where applicable.	The section aims to protect children from all harm and abuse, this is commendable and a prerequisite for any law. The requirement of verifiable parental consent is a welcome step however should be required only for individuals ages 13 and under referred to as 'child'. (Please see definition clause 2(3) as suggested.) There is no need for parental consent for individuals aged 13-18 or teenagers. (Please see definition clause 2(3) as suggested.) CUTS' study found that users in this age bracket avail various popular data-driven online services and parents are comfortable with their ward availing services without their permission. Further, CUTS found that parents believe that their child knows more than them about safe online practices to adopt, and is capable of providing consent. [58] There is a need to adopt age verification technologies

[58] Kulkarni, Amol et.al. 'Protecting Children's Data: Analysing Perspectives of Parents & Children' *available at* https://cuts-ccier.org/pdf/slide-deck-protecting-childrens-data-analysing-perspectives-of-parents-children.pdf

			which are least intrusive to protect young users from problematic experiences online, such as cyber-bullying/stalking, exposure to problematic content etc.[59]
10. (3)	A Data Fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.	A Data Fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children **except for the purpose of implementing child safety measures to protect children from problematic experiences online.** **For the purpose of this subsection, problematic experiences shall include cyber-bullying/stalking, exposure to problematic content like pornography, cruelty, etc.**	A complete restriction on tracking and behavioural monitoring of children or targeted advertising might be counter-productive to child safety measures. CUTS' study found that over 75 percent of parents, and 55 percent of young users are comfortable with Data Fiduciaries tracking and monitoring the online behaviour of young users, but only for the valid objective of ensuring their online safety. Many parents and young users are also comfortable with service providers blocking inappropriate content for children. This requires online age verification and behavioural tracking of children. Adequate safeguards with respect to purpose limitation and data minimisation should be incorporated into the law.[60]
10. (4)	The provisions of sub-sections (1) and (3) shall not be applicable to processing of personal data of a child for such purposes, as may be prescribed.	**This subsection should be deleted.**	See suggestions for 10(1) and (3). These make this clause redundant.
11. Additional obligations of Significant Data Fiduciary			
11. (1)	The Central Government may	The Central Government may notify	Notification of Significant Data Fiduciaries should be

[59] *Ibid.*
[60] *Ibid.*

	notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, on the basis of an assessment of relevant factors, including: (a) the volume and sensitivity of personal data processed; (b) risk of harm to the Data Principal; (c) potential impact on the sovereignty and integrity of India; (d) risk to electoral democracy; (e) security of the State; (f) public order; and (g) such other factors as it may consider necessary;	any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, on the basis of a **transparent process of Scientific Risk Assessment** of relevant factors, including: (a) the volume and sensitivity of personal data processed; (b) risk of harm to the Data Principal; (c) potential impact on the sovereignty and integrity of India; (d) risk to electoral democracy; (e) security of the State; **and** **(f) xx** **(g) xx** **(f) existing state of data security, privacy policy implemented by Data Fiduciary, and vulnerability of data breach in relation to Data Fiduciary.** **For the purpose of this section, Scientific Risk Assessment shall include conducting a consultation with all relevant stakeholders including the Board, law enforcement agencies, subject matter experts, civil society and consumer organisations. The assessment will be done in a**	subjected to adequate stakeholder consultation, and scientific risk assessment. This may be developed by taking factors such as the existing state of data security, privacy policy, vulnerability of data breach into account. Undertaking security risk assessment and transparent consultation will ensure informed decision-making for consumers (or their representatives) and other stakeholders such as Significant Data Fiduciaries and Law Enforcement Agencies (LEAs). While consultation and scientific risk assessment is essential, it should be transparent, and an opportunity of hearing must be provided to the entity/ entities under question. Decisions along with reasons should also be available in the public domain to infuse trust and transparency in the process. Affected Data Fiduciaries who have been classified as Significant Data Fiduciaries should have the Right to appeal against the decision. Further, all decisions made with respect to making such classifications should be reviewed periodically and affirmed, failing which the entity should be reverted to be treated as Data Fiduciary. Inspiration can be drawn from designation of systemically important entities by the financial sector regulators such as the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI). Moreover, this section also includes grounds such as "public order" and "such other factors as it may consider necessary" which have ambiguity and can be misused.

		transparent manner and the process followed should be made available in the public domain. **New subsections to be inserted as subsections 11(1A) and 11(1B):** **11(1A). This decision of the Central Government shall be contestable in the Court by the entity(s) which has been regarded as Significant Data Fiduciary. An opportunity of hearing shall be provided to the entity(s), and the order of such hearing along with the rationale shall be made available in the public domain.** **11(1B). All decisions made with respect to classifying a Data Fiduciary as Significant Data Fiduciary shall be subject to periodic reviews.**	Therefore, these terms must be explicitly defined, or else should be removed as similar provisions in other laws have been repeatedly misused by the Executive for shutting down the Internet.[61] For example, for conducting several competitive examinations, the Internet was shut down despite no such threat.[62]
11. (2) (a)	appoint a Data Protection Officer who shall represent the Significant Data Fiduciary	appoint a Data Protection Officer who shall represent the Significant Data Fiduciary under the provisions of this	The proposed provision fails to clearly define the role and responsibilities of a Data Protection Officer (DPO) and a grievance officer. Moreover, the proposed provision

[61] 'Explained: The frequency, reasons, and controversy over Internet suspensions by the government' *available at* https://indianexpress.com/article/explained/explained-the-frequency-reasons-and-controversy-over-internet-suspensions-by-the-government-8005450/
[62] Internet Shutdown Tracker, *available at* https://internetshutdowns.in/

	under the provisions of this Act and be based in India. The Data Protection Officer shall be an individual responsible to the Board of Directors or similar governing body of the Significant Data Fiduciary. The Data Protection officer shall be the point of contact for the grievance redressal mechanism under the provisions of this Act;	Act and be based in India. The Data Protection Officer shall be an individual responsible to the Board of Directors or similar governing body of the Significant Data Fiduciary. **There shall be** a clear point of contact for the grievance redressal mechanism under the provisions of this Act; **New subsection to be inserted as subsections 11 (2) (d) and (e):** **(d) shall periodically publish reports on any data breaches, complaints received and action taken and/ or not taken in pursuance of the complaint or grievance received by it on the same; and** **(e) shall provide intimation about changes in privacy policy, data collection and processing practices in clear, concise and plain language which is easily comprehensible to a reasonable person.**	mandates the DPO to ensure compliance and redress Data Principal grievances. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021)[63] which has similar provisions has clearly defined the same. CUTS recommends that the roles and responsibilities of the Significant Data Protection Officer and grievance officer be clearly defined for transparency and accountability in the grievance redressal process. To maintain transparency, CUTS recommends that Significant Data Fiduciary should periodically publish reports on any data breaches, grievances received and action taken and/ or not taken in pursuance of the complaint or grievance received by it on the same. Data Principal should be intimated in changes related to notices, data collection and processing practices.[64]
Chapter 3: RIGHTS & DUTIES OF DATA PRINCIPAL			

[63] 'Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021' *available at* https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf

[64] 'Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021' *available at* https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf

12. Rights to information about personal data			
12. (1)	The Data Principal shall have the right to obtain from the Data Fiduciary: (1) the confirmation whether the Data Fiduciary is processing or has processed personal data of the Data Principal;	**Withdraw. Subsumed within newly inserted Section 9(11).**	See suggested Section 9(11).
12. (2)	a summary of the personal data of the Data Principal being processed or that has been processed by the Data Fiduciary and the processing activities undertaken by the Data Fiduciary with respect to the personal data of the Data Principal;	**Withdraw. Subsumed within newly inserted Section 9(11).**	See suggested Section 9(11).
12. (3)	The Data Principal shall have the right to obtain from the Data Fiduciary: in one place, the identities of all the Data Fiduciaries with whom the personal data has been shared along with the categories of personal data so shared; and	The Data Principal shall have the right to obtain, **by way of a request, in a reasonable time** from the Data Fiduciary: **a) in one place, the identities of all the Data Fiduciaries with whom the personal data has been shared along with the categories of personal data so shared; and**	The rights given to the data principal for obtaining information is a welcome move. However, there is a lack on how the data principal can avail this right. Therefore, the section should provide for the mode of availing these rights and the information requested for by the data principal should be provided to her in a reasonable and justified time.

		b) details for section 9 subsection 11.	
13. Right to correction and erasure of personal data and *Right to be Forgotten*			
13. (3)	**Insertion of New Clause - Right to be Forgotten**	**The Data Principal shall have the right to stop and prevent the continuing disclosure or processing of her personal data by a Data Fiduciary where such disclosure or processing:** **(a) has served the purpose for which it was collected or is no longer necessary for the purpose;** **(b) was made with the explicit consent of the data principal and such consent has since been withdrawn; or** **(c) was made contrary to the provisions of this Act or any other law for the time being in force.**	The draft Bill does away with the provision of the Right to be Forgotten present in the DPB'21 given by the JPC. To protect the privacy of the Data Principal, she should be given under Right to be Forgotten.[65] CUTS recommends that Right to be Forgotten should be inserted in the draft Bill as it will give more control to the Data Principal over their data.
14. Right of grievance redressal			
14. (1)	A Data Principal shall have the right to readily available means	A Data Principal shall have the right to readily available, **trustworthy, user**	The term 'readily available means' is unclear. Furthermore, to make grievance redressal mechanisms

[65] Report of Joint Parliamentary Committee on Personal Data Protection Bill, 2021, *available at* https://drive.google.com/file/d/1emcAB8HjE2oCC_DI6zR5YPnPQ5iwwwCT/view

	of registering a grievance with a Data Fiduciary.	**friendly, and cost-effective** means of registering a grievance with a Data Fiduciary.	accessible, effective, trustworthy, and user friendly, the draft should mandate service providers to provide alternate grievance redressal mechanisms including leveraging existing online and alternate dispute resolution and consumer assistance centres. Moreover, like IT Rules, 2021[66], the draft Bill may consider defining types of grievances such as violation of privacy, processing of personal data without consent, harms and data breaches which can be lodged. Initiatives such as CUTS' Grahak Sahayata Kendra should be adopted,[67] given that they can act as a mediator and conciliator between consumers and Data Fiduciaries. Data Principals should be allowed to lodge complaints or seek information and clarifications via toll-free numbers, online portals, emails, or in-person.[68] To build capacity among consumers, along with consumer organisations, local nodes of information providers such as community radio, multilingual local newspapers can be used.
14. (2)	A Data Principal who is not satisfied with the response of a Data Fiduciary to a grievance or receives no response within seven days or such shorter period as may be prescribed,	A Data Principal who is not satisfied with the response of a Data Fiduciary to a grievance or receives no response within seven days or such shorter period as may be prescribed, may register a complaint with the Board in	Informed by the Consumer Protection Act 2019, a timeline of not more than 60 days may be provided for resolutions of complaints at the level of the Data Protection Board.[69] Also, the draft Bill may introduce mediation mechanisms along the lines of CUTS Grahak

[66] 'Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021' *available at* https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf

[67] Grahak Sahayata Kendra, *available at* https://cuts-cart.org/consumer-support-centre-grahak-sahayta-kendra/

[68] CUTS Submission to the Joint Committee on The Personal Data Protection Bill, 2019, *available at* https://cuts-ccier.org/pdf/submission-pdpb-2019.pdf

[69] Consumer Protection Act, 2019, *available at* https://egazette.nic.in/WriteReadData/2019/210422.pdf

	may register a complaint with the Board in such manner as may be prescribed.	such manner as may be prescribed. **The Board should resolve the complaints within a period of sixty days.**	Sahayata Kendra.[70] The same is recommended in the suggestions made under Section 23.
14. (3)	**Insertion of New Clause**	**Any person who has suffered tangible and/ or intangible damage as a result of a contravention of this law shall have the right to receive compensation from the Data Fiduciary for the damage suffered. This also includes personal data breach, resulting in any tangible and intangible harms.**	Unlike the previous draft versions of the Bill, this version does not provide Data Principals with the right to claim compensation. The draft should include such a right in case consumers suffer from any kind of harm due to the Data Fiduciaries violating the law and/ or in case of data breaches. The draft should also explicitly provide clarification on definitional components of harm. In case of harm caused and subsequent right to claim compensation, Data Principals should have the right to involve consumer organisations to assist them. In addition, mere contravention of provisions of the Act should be sufficient for Data Principals to file a complaint, whether or not resulting in associated harm. Lastly, the procedure for seeking compensation must be accessible and understandable to consumers. CUTS study[71] pointed out that not many consumers who experienced a personal data breach or a privacy violation, did not complain about it, since they were unaware of avenues of registering their grievances.[72] Accordingly, setting up consumer assistance centres, tasked with building capacity, and facilitating grievance redress for consumers is important.

[70] Grahak Sahayata Kendra, *available at* *https://cuts-cart.org/consumer-support-centre-grahak-sahayta-kendra/*
[71] 'Users' Perspectives On Privacy And Data Protection' *available at* Https://Cuts-Ccier.Org/Pdf/Survey_analysis-Dataprivacy.Pdf
[72] 'Users' Perspectives On Privacy And Data Protection' *available at* Https://Cuts-Ccier.Org/Pdf/Survey_analysis-Dataprivacy.Pdf

15. Right to nominate.			
15.	A Data Principal shall have the right to nominate, in such manner as may be prescribed, any other individual, who shall, in the event of death or incapacity of the Data Principal, exercise the rights of the Data Principal in accordance with the provisions of this Act. For the purpose of this section, "incapacity" means inability to exercise the rights of the Data Principal under the provisions of this Act due to unsoundness of mind or body	A Data Principal shall have the right to nominate **and/ or right to be forgotten as defined under the clause 13(3)**, in such manner as may be prescribed, any other individual, who shall, in the event of death or incapacity of the Data Principal, exercise the rights of the Data Principal in accordance with the provisions of this Act. **In the absence of any nomination, lawful heirs of the deceased may exercise the rights provided in this Act.** For the purpose of this section, "incapacity" means inability to exercise the rights of the Data Principal under the provisions of this Act due to unsoundness of mind or body	Without any nomination, the draft should prescribe that the heirs of the deceased may exercise the rights provided in the Bill. Further, the deceased Data Principals should be given the right to be forgotten, and append the terms of the agreement regarding processing of personal data in the event of the Data Principal's death.
16. Duties of Data Principal.			
16. (1)	A Data Principal shall comply with the provisions of all applicable laws while exercising rights under the provisions of this Act.	**This Clause should be withdrawn.**	It should be obvious and if the draft Bill intends otherwise, it should be clearly stated. There is no requirement for this clause and it should be deleted.

16. (2)	A Data Principal shall not register a false or frivolous grievance or complaint with a Data Fiduciary or the Board.	**This Clause should be withdrawn. Correspondingly, also withdraw Schedule 1 (5).**	Promoting a practice where consumers are not indulging in false and frivolous complaints is important. However, imposing a penalty of INR 10,000 on non-compliance (as mentioned in the Schedule 1 of the draft Bill) with this might discourage consumers from registering their legitimate grievances. This should be withdrawn as it might act as a deterrent for aggrieved consumers while those who will be habitual offenders in registering false complaints might not shy from giving penalties of INR 10,000.
16. (3)	A Data Principal shall, under no circumstances including while applying for any document, service, unique identifier, proof of identity, or proof of address, furnish any false particulars or suppress any material information or impersonate another person.	**This Clause should be withdrawn.**	This is laudable as it prohibits consumers from furnishing any false particulars, suppressing any material information (remains to be appropriately defined in the draft Bill), or impersonating another person while applying for any document, service, unique identifier, proof of identity, or proof of address. However, it overlaps with prohibition under the Indian Penal Code (IPC). IPC already deals with such cases[73], such as sections 419 (cheating by impersonation), 420 (cheating), 467 (forgery), 468 (forgery for cheating), and 471 (fraudulently or dishonestly using a genuine document) are notable in this regard. Given that such issues are dealt with by LEAs, under the IPC, the need for having such provisions under this draft Bill seems unnecessary. Therefore, this provision should be removed by appropriately incorporating it under the IPC.
16. (4)	A Data Principal shall furnish only such information as is	A Data Principal shall furnish **only as much information as is required and**	The requirement of 'verifiably authentic' information in correction and erasure should be defined in explicit terms

[73] The Indian Penal Code, *available at*: https://legislative.gov.in/sites/default/files/A1860-45.pdf

	verifiably authentic while exercising the right to correction or erasure under the provisions of this Act.	**such** as is verifiably authentic while exercising the right to correction or erasure under the provisions of this Act.	and should not be linked to any official identification proofs. The process should strictly adhere to the principle of minimum data collection.
Chapter 4: SPECIAL PROVISIONS			
17. Transfer of personal data outside India			
17. (1)	The Central Government may, after an assessment of such factors as it may consider necessary, notify such countries or territories outside India to which a Data Fiduciary may transfer personal data, in accordance with such terms and conditions as may be specified.	**The Central Government in consultation with the Board may notify such countries or territories outside India to which a Data Fiduciary may transfer personal data, in accordance with such terms and conditions as may be specified, after an assessment of factors including:** **(a) level of data protection in other countries;** **(b) ability of Data Principal to exercise their rights;** **(c) accessibility of transferred data to Indian law enforcement agencies; and** **(d) strategic and foreign policy considerations.**	The draft Bill has omitted the requirement of storing data within the Indian national boundaries which is a welcome step. The draft Bill states that the government may, after the assessment, notify the territories where data can be transferred. However, the grounds for the evaluation remain unclear. The draft Bill should prescribe the requirements and transparent standards such as the level of data protection in other countries, the ability of consumers to exercise their rights, efficiency gains to Data Fiduciaries, comfort of law enforcement agencies, and strategic and foreign policy considerations for transferring data outside India.
17. (2)	**Insertion of New Clause**	**Before issuing any notification under subsection 17(1), the Central**	Consumer Impact Assessment study of CUTS underscored the unintended impact of data localisation

		Government, in consultation with the Board, shall undertake the following steps: **(a) perform a cost-benefit analysis;** **(b) conduct a public consultation where all relevant stakeholders are invited; and** **(c) record reasons in writing for excluding any countries or territories outside India.**	(DL) on users in terms of possible reduced uptake of select data-driven services while adversely impacting the availability of services and curbing innovation. Further, the study suggests that DL can increase the risks of privacy violation, cyber-attacks and data breaches.[74] CUTS study on the impact of Data Localisation on Digital Trade shows that it will negatively impact trade and innovation while increasing the compliance cost.[75] Before prescribing territories where personal data can be transferred and/or disallowed to transfer, CUTS recommend that the Central Government in consultation with the Board must undertake a Cost-Benefit Analysis (CBA). Undertaking CBA for this will ensure that the costs imposed by restriction do not outweigh its intended possible benefits, not only for the consumers but also for other stakeholders such as service providers. Additionally, the findings of such CBA should be published in the public domain to maintain transparency and trust.
18. Exemptions			
18. (1)	The provisions of Chapter 2 except sub-section (4) of section 9, Chapter 3 and Section 17 of this Act shall not apply where:	The provisions of Chapter 2 except sub-section (4) of section 9, Chapter 3 and Section 17 of this Act shall not apply where, any data fiduciary seeks permission for the same by **making a written request to a designated**	Previous versions of the Bill provided some procedural safeguards in this regard. For example, the PDPB'19 required exemption orders to be subject to a 'procedure, safeguards and oversight mechanism', while the DPB'21 required orders to be 'just, fair, and reasonable'. As per the Puttaswamy Judgment of the Supreme Court, any

[74] 'Consumer Impact Assessment on Cross-Border Data Flow' *available at* https://cuts-ccier.org/consumer-impact-assessment-on-cross-border-data-flow/
[75] Understanding Impact of Data Localization on Digital Trade, *available at* https://cuts-ccier.org/understanding-impact-of-data-localization-on-digital-trade/

	(a) the processing of personal data is necessary for enforcing any legal right or claim; (b) the processing of personal data by any court or tribunal or any other body in India is necessary for the performance of any judicial or quasi-judicial function; (c) personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law; (d) personal data of Data Principals not within the territory of India is processed pursuant to any contract entered into with any person outside the territory of India by any person based in India.	**competent judicial/executive authority, clearly stating:** **i) reasons and time period for seeking the exemption;** **ii) time period and reasons for said time period for exemption;** **iii) sections of the Act from which exemptions are sought and reasons thereof, for the purposes of;** (a) the processing of personal data is necessary for enforcing any legal right or claim; (b) the processing of personal data by any court or tribunal or any other body in India is necessary for the performance of any judicial or quasi-judicial function; (c) personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law; (d) personal data of Data Principals not within the territory of India is processed pursuant to any contract entered into with any person outside	exemption made to the Central Government should be subjected to three pronged tests of legality, necessity and proportionality.[76] Also, sub-clause (c) prevention as a ground for exemption is too broad and should have stricter restrictions in order to safeguard the interests of digital nagriks. No data fiduciary should be able to get away from their obligations and data principals rights must not be waived without any judicial oversight mechanism or senior executive authority's reasoned orders. All exemptions should be allowed through a judicial/executive order to prevent the misuse of exemptions. A judicial committee must be empowered to examine the merit of the exemption. This will be an extension of the judicial review, which is a constituent of the basic structure of the constitution.[77] Provisions related to judicial review of orders to process data exist in jurisdictions abroad. The UK Supreme Court, in a landmark case,[78] ruled that "government security decisions will in future be open to challenge in the courts".[79]

[76] Justice K S Puttaswamy (Retd.) and Another Vs. Union of India and Others SC WP(C) No. 494 of 2012.
[77] Indira Gandhi v. Raj Narain, 1976 (2) SCR 347.
[78] R (on the application of Privacy International) v. Investigatory Powers Tribunal and others, UKSC 2018/0004 *available at* R (on the application of Privacy International) (Appellant) v Investigatory Powers Tribunal and others (Respondents)
[79] UK government security decisions can be challenged in court, judges' rule | GCHQ | The Guardian

		the territory of India by any person based in India. **In case such exemption is challenged, the burden of proof shall lie on data fiduciary.**	Also, to protect the fundamental right of privacy, prescriptions for the right to legal recourse against data processing under government exemptions should be made in the law itself. Though overly prescriptive legislation is discouraged, adding the prescription in the law would also ensure one aspect of the procedural safeguards necessary to meet the test of proportionality and, by extension, the test of privacy. Also, inclusion of a justified and reasonable time period and restricting the data processing to not be continuous in nature will protect the rights of Data Principals.
18. (2)	The Central Government may, by notification, exempt from the application of provisions of this Act, the processing of personal data: a. by any instrumentality of the State in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these; and	The Central Government may, by **making a written request to a designated competent judicial/executive authority, clearly stating:** **i) reasons for seeking the exemption;** **ii) time period and reasons for said time period for exemption;** **iii) sections of the Act from which exemptions are sought,** exempt from the application of provisions of this Act, the processing of personal data: a. by any instrumentality of the State in **situations where a substantial risk**	The use of terms such as 'public order', 'interest of state' should not be used for exemptions unless there exists any substantial risk to the same. Such terms are susceptible to misuse and have deep impacts on the freedom of Data Principals. There is usually an inter-connection between 'public order, 'law and order,' and 'security of the state.'[80] The term 'public order' has a wide definition and the limitation imposed in the interests of public order needs to be a reasonable restriction. It is necessary that it has a proximate connection or nexus with public order and not be far-fetched, hypothetical or problematic, or too remote in the chain of its relationship with the public order.[81]

[80] Dissent Note of Jairam Ramesh, JPC Report Pg. 240 *available at* http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

[81] The Superintendent, Central Prison, Fatehgarh v. Ram Manohar Lohia, 1960 AIR 633, 1960 SCR (2) 821.

	(b) necessary for research, archiving or statistical purposes if the personal data is not to be used to take any decision specific to a Data Principal and such processing is carried on in accordance with standards specified by the Board.	**exists to** interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these; and (b) necessary for research, archiving or statistical purposes if the personal data is not to be used to take any decision specific to a Data Principal and such processing is carried on in accordance with standards specified by the Board. **In case such exemption is challenged, the burden of proof shall lie on data fiduciary.**	The term public order is too broad and empowers the Central Government to process such personal data for reasons beyond what it is collected for. Further, exemptions based on executive order are contrary to the requirements stated in the Puttaswamy judgement, wherein executive notifications were held to be insufficient for restricting the fundamental right to privacy.[82] Notably, the government acknowledged the lack of a specific definition of public safety and public emergency last year to the Parliament's Standing Committee on Communications and Information Technology.[83] Accordingly, such terms must be defined in the draft Bill and exemption sought by government agencies should be given only if they fulfil the requirements of legality, necessity, and proportionality. In this regard, the Asia Pacific Economic Cooperation (APEC) privacy framework also specifies limitations for use only for the objectives of exemptions.[84] Further, the Bill should require the government to conduct a cost-benefit analysis to assess if benefits outweigh the cost of exercising exemptions.[85] Further, similar conditions of an oversight mechanism and time and purpose limitation as suggested for Section 18 (1) should be applicable.

[82] Justice K.S. Puttaswamy (Retd) vs Union of India, (2019).
[83] 'No clear public safety, emergency definition: Net ban being used for routine policing', *available at:* https://indianexpress.com/article/technology/no-clear-public-safety-emergency-definition-net-ban-beingused-for-routine-policing-7651616/
[84] Part ii (13) APEC Privacy Framework.
[85] Heda, Shubhangi, 'Exemptions for the State', *available at* Exemptions for the State

18. (3)	The Central Government may by notification, having regard to the volume and nature of personal data processed, notify certain Data Fiduciaries or class of Data Fiduciaries as Data Fiduciary to whom the provisions of Section 6, sub-sections (2) and (6) of section 9, sections 10, 11 and 12 of this Act shall not apply.	The Central Government may by **way of reasoned orders available in public domain,** having regard to the volume and nature of personal data processed, notify certain Data Fiduciaries or class of Data Fiduciaries as Data Fiduciary to whom the provisions of Section 6, sub-sections (2) and (6) of section 9, sections 10, 11 and 12 of this Act shall not apply. **For the purpose of this section: reasoned orders shall contain appropriate reasons and period of time for exemption.**	The nature of these exemptions is quite ambiguous which generates the fear of misinterpretation and misuse. The draft Bill should mandate stakeholder consultation for exemption given to the Government and its agencies. The Government's powers should be subject to a consultative process and the final report of the same should be put in public domain to infuse trust and transparency. Moreover, in compliance with the Puttaswamy judgement, the draft Bill should require the Government to justify that the order exempting its agency from the draft Bill complies with the principles of legality, necessity, and proportionality. In this regard, the Government must be required to undertake a cost-benefit analysis and release its findings in the public domain to justify that the costs of its action are outweighed by the benefits.
18. (4)	The provisions of sub-section (6) of section 9 of this Act shall not apply in respect of processing by the State or any instrumentality of the State	**This Clause should be withdrawn.**	The proposed provision of the draft Bill has increased the scope of the state exemption which can have an adverse impact on consumers freedom and privacy. The rationale behind choosing these proposed provisions for exemption have not been provided. Also, Section 9(6) restricts retention of data and this sub-clause exempts it for state and instrumentalities of the state. This is potentially unconstitutional. Further, the Bill should require the government to conduct a cost-benefit analysis to assess if benefits outweigh the cost of exercising exemptions and also the cost of retaining data for an unspecified period of time.[86]

[86] Exemptions for the State

			Further, the subsection is open ended and ambiguous in nature and can also be done under subsection (2) and therefore should be withdrawn.
Chapter 5: COMPLIANCE FRAMEWORK			
19. Data Protection Board of India			
19. (2)	The strength and composition of the Board and the process of selection, terms and conditions of appointment and service, removal of its Chairperson and other Members shall be such as may be prescribed.	The strength and composition of the Board and the process of selection, terms and conditions of appointment and service, removal of its Chairperson and other Members shall be such as may be prescribed**, while incorporating the following principles:** **(a) The Central Government shall provide a list of suitable candidates after advertising the vacancy for positions for the Board and inviting such candidates as it may feel suitable for the positions after recording reasons in writing.** **(b) Parliament will be involved by**	The Clause 19 (2) allows the Central Government to decide and alter the composition of the Board including choosing the chief executive and deciding the tenure of the members, among other things. The clause does not lay down the selection procedure to be followed and states that it will be prescribed later on. As the Central Government itself is one of the largest Data Fiduciaries and Data Processors, it being empowered to make appointments to the Board which will perform adjudicatory functions, leads to the risk of conflict of interest. This will diminish the independence of the Board. Additionally, as per the Section 20, the Board will be performing many investigative and adjudicatory functions. As per the Madras Bar Association[87] case and the Rojer Mathews[88] case, the Supreme Court has stated that the judicial functions cannot be performed by

[87] Madras Bar Association versus Union of India, 2014 (308) ELT209 (S.C.), Supreme Court of India, September 25, 2014, *available at:* https://main.sci.gov.in/judgment/judis/41962.pdf

[88] Rojer Mathew versus South Indian Bank Ltd & Ors., 2019 (369) ELT3 (S.C.), Supreme Court of India, November 13, 2019, *available at:* https://www.sci.gov.in/pdf/JUD_4.pdf

		the way of the Standing Committee nominating the members to be appointed to the Board after conducting a hearing of the list of suitable candidates. **(c) Board shall comprise at least one expert in the field of data protection, cyber and internet laws, consumer protection and related subjects. For performing the adjudicatory functions, the Board will have at least one Member with judicial background such as former judges of the Supreme Court or the High Court. Board may also comprise persons working in other regulatory authorities in or outside India.** **(d) The rejected candidates shall have the opportunity of being heard and challenging the selection decision in the Court.** **(e) The entire procedure must be fair, transparent, and efficient by incorporating methods such as the Standing Committee live streaming all proceedings of hearing of candidates and publishing a report on the entire proceeding highlighting the reasons for the**	technical members.[89] Given the Board has adjudicatory functions, the composition of the Board should include former judges of the Supreme Court or the High Court. In the interest of protecting the independence and sovereignty of the Board (as is mentioned in Clause 21(1)) and upholding accountability and transparency in the appointment process, the clause should lay down the principles, utilising which, the process of selection, terms and conditions of appointment and service, removal of its Chairperson and other Members shall be prescribed. These principles should address the above-mentioned issues. The selection of the Board should include the Parliamentary Standing Committee on Information Technology (IT) for making the entire process more robust and democratic. The Central Government should invite applications through advertisements and consider non-applicant persons after recording reasons in writing. Experts in the field of data protection, cyber and internet laws, consumer protection and related subjects and persons working in other regulatory agencies and authorities, in or outside India, must be invited to apply for the position. The candidates shortlisted by the Central Government should be finally heard by the Parliamentary Standing Committee on Communications and IT and appointment of the finally selected candidates can be made by the President.

[89] The Tribunal System in India, PRS Legislative Research, *available at*: https://prsindia.org/files/bills_acts/bills_parliament/2021/Note%20-%20Tribunal%20system%20in%20India.pdf

		decisions made. The procedure should be completed in a time-bound manner in a period of a maximum of ninety days. **(f) The Members of the Board to be subject to a cooling-off period of 2 years.** **For the purposes of this subsection, Standing Committee means Parliamentary Standing Committee on Communications and Information Technology.**	The process should be completed in a period of 90 days in a fair, transparent and efficient manner. Measures which bring in transparency and accountability should be incorporated. For this purpose, all proceedings can be live streamed with reasoned decisions for the selection made should be made public in a report format. The opportunity of being heard and challenging the selection decision in the Court should be provided.
19. (4)	The Board shall have such other officers and employees, with such terms and conditions of appointment and service, as may be prescribed.	The Board shall have such other officers and employees, with such terms and conditions of appointment and service, as may be **decided by the Board, for meeting its the requirements of its day-to-day operations.**	In order to protect the independence of the Board, the power to make appointments of other officers and employees, by stating the terms and conditions of appointment and service, should be given to the Board.
20. Functions of the Board			
20. (1)	The functions of the Board are: (a) to determine non-compliance with provisions of this Act and impose penalty under the provisions of this Act; and	**The Board will have investigative and adjudicatory powers and shall** determine non-compliance with provisions of this Act and impose penalty under the provisions of this Act**.**	As per the Clause 20(1) (a), the functions of the Board have been limited to only determining non-compliance with provisions under the Bill and imposing corresponding penalties. Under Section 26, the Central Government is empowered to make Rules to carry out the provisions of the Act. This effectively leaves the Board to

	(b) to perform such functions as the Central Government may assign to the Board under the provisions of this Act or under any other law by an order published in the Official Gazette.		be an authority which will be performing investigative and adjudicatory functions. The Board has not been given powers to perform regulatory functions. Further, as per the Clause 20(1)(b) the Central Government may assign other functions to the Board 'by an order published in the Official Gazette'. In the context of the Board being an independent authority, it should be noted that the 'by an order published in the Official Gazette' is excessive delegation to the Central Government and orders released under this will be substantively ultra-vires and thus should be removed. The Board should derive its power from the parent law and not a delegated legislation in the form of an executive order.
20. (5)	**Insertion of New Clauses**	**The Board may, for effectively and efficiently performing its functions under the Act, may also perform additional functions as may be required, including:** **(a) promoting awareness and understanding of the risks, rules, safeguards and rights in respect of protection of personal data amongst Data Fiduciaries, Data Processors and Data Principals in English or any language specified in the Eighth Schedule to the Constitution of India;** **(b) easing the mechanisms of grievance redressal and seeking**	The Board should also perform such positive obligatory functions, which may be necessary to effectively and efficiently perform the investigative and adjudicatory functions. The Board should function in a manner that it does not disable any Data Principal including those from the vulnerable sections of the society from approaching it in case their rights under the Bill are violated. Accordingly, while choosing to operate digitally or physically, the Board should ensure ease to Data Principals in aspects like filing grievances and seeking clarifications, among others. Further, the Board should also utilise regional languages to ensure that larger populations can access grievance redressal mechanisms in their own language. The Board can garner help from civil society and consumer organisations.

		clarification for Data Principals; **(c) maintaining a database on its website containing names of significant Data Fiduciaries;** **(d) promoting measures and supporting and undertaking research for innovation in the field of protection of personal data;** **(e) coordinating with other regulators, civil society and consumer organisations and soliciting feedback on actions to be taken or already taken;** **(f) protecting whistle-blowers and awarding bounties;** **(g) advising Central Government, State Government and any other authority on measures required to be taken to promote protection of personal data and ensuring consistency of application and enforcement of this Act;** **(h) performing such other functions that enable the Board to act proactively to ensure welfare and protection of rights for all individuals; and** **(i) periodically reporting all activities undertaken by the Board.**	The Board must also ensure that there is ease of providing feedback for the public consultation, for all policy documents it releases. To uphold accountability and transparency, the Board must also periodically report the steps taken to ensure compliance with these aspects. The draft Bill must specify more functions of the Board, including promoting awareness and understanding of the risks, rules, safeguards and rights in respect of protection of personal data; protecting whistle-blowers and awarding bounties; advising Central Government, State Government and any other authority on measures required to be taken to promote the protection of personal data and ensuring consistency of application and enforcement of this Act; and such other functions enable the Board to act proactively to protect individual' rights.
21. Process to be followed by the Board to ensure compliance with the provisions of the Act			

21. (3)	The Board may authorise conduct of proceedings relating to complaints, by individual Members or groups of Members.	The Board may authorise conduct of **investigative and adjudicative** proceedings relating to complaints by**:** **(a) an Investigation Wing having designated Inquiry Officer(s), who shall be employees of the Board, to perform the investigative functions. Such Inquiry Officer(s) shall have a fixed term of one year or as may be prescribed by the Board; and** **(b) individual Members or groups of Members of the Board to perform the adjudicatory functions, of whom at least one has a judicial background**.	The term 'conduct of proceedings' may include both investigative and adjudicatory function. There is a need to clearly demarcate the performance of such functions and different members should conduct them. In this regard, for performing investigative functions, the Board must have a separate Investigation Wing, in order to avoid any potential conflict of interest. Accordingly, under clause 21(3), the Board should designate an Inquiry Officer(s) with fixed term to conduct the investigative proceedings to ensure that they are carried out independently and impartially, without any undue influence. Further, with respect to performing adjudicatory functions, it is necessary for the Board to have at least member with a judicial background, in compliance with the requirements laid down in the Madras Bar Association[90] case and the Rojer Mathews[91] case by the Supreme Court.
21. (4)	The Board shall first determine whether there are sufficient grounds to proceed with an inquiry. In case the Board determines that there are insufficient grounds, it may, for reasons recorded in writing,	The Board shall first determine whether there are sufficient grounds to proceed with an inquiry. In case the Board determines that there are insufficient grounds, it may, for reasons recorded in writing, close such proceedings. **The reasoned order will**	Under Clause 21(4), while closing down proceedings on insufficient grounds is desirable, the reasons recorded in writing should be made publicly available, so that interested parties including the data principal(s), know the cause for the closure of proceedings. This is necessary to uphold the principles of transparency and accountability.

[90] Madras Bar Association versus Union of India, 2014 (308) ELT209 (S.C.), Supreme Court of India, September 25, 2014, *available at:* https://main.sci.gov.in/judgment/judis/41962.pdf
[91] Rojer Mathew versus South Indian Bank Ltd & Ors., 2019 (369) ELT3 (S.C.), Supreme Court of India, November 13, 2019, *available at:* https://www.sci.gov.in/pdf/JUD_4.pdf

	close such proceedings.	**be made publicly available.**	
21. (7)	For the purpose of conduct of inquiry under this section, the Board shall have powers to summon and enforce the attendance of persons, examine them on oath and inspect any data, book, document, register, books of account or any other document.	For the purpose of conduct of inquiry under this section, **the Inquiry Officer(s) in the Investigation Wing appointed by** the Board shall have powers to summon and enforce the attendance of persons, examine them on oath and inspect any data, book, document, register, books of account or any other document.	The powers given to the Board under Clause 21 (7) should be given to the Inquiry Officer(s) in the Investigation Wing, appointed by the Board (as per the suggestion made in Clause 21(3)). This is essential to ensure that the investigation and adjudication processes are carried out independently. If the same person performs both investigative and adjudicatory functions, the judgement in the adjudication process may get affected as the person concerned may pre-empt their decision.
21. (11)	On conclusion of the inquiry and after giving the concerned persons a reasonable opportunity of being heard, if the Board determines that non-compliance by a person is not significant, it may, for reasons recorded in writing, close such inquiry. If the Board determines that the non-compliance by the person is significant, it shall proceed in accordance with section 25 of this Act.	On conclusion of the inquiry and after giving the concerned persons a reasonable opportunity of being heard, **the Board may do the following:** **(a) if the Board determines that non-compliance by a person is not significant, it may, for reasons recorded in writing, close such inquiry.** **(b) if the Board determines that the non-compliance by the person is significant, it shall proceed in accordance with section 25 of this Act. Additionally, the Board may also issue specific performance orders to persons involved, as may be required to ensure compliance with the provisions of the Act.**	As per the Section 25, the Board can only impose financial penalty. This may prevent the Board from issuing orders mandating compliance with the law. It is critical to ensure that relevant parties take necessary actions to comply with the law and ensure that adverse impact on all parties is arrested. Accordingly, under Clause 21 (11), the Board should be empowered to issue specific performance in relation to obligations of relevant parties and impose such orders which may be required to ensure compliance with the provisions of the Bill.

21. (12)	At any stage after receipt of a complaint, if the Board determines that the complaint is devoid of merit, it may issue a warning or impose costs on the complainant.	At any stage after receipt of a complaint, if the Board determines that the complaint is devoid of merit, **after providing reasonable opportunity of being heard to the complainant, and for reasons recorded in writing,** it may issue a warning or impose costs on the complainant.	Under Clause 21 (12), the Board should provide reasonable opportunity of being heard to the complainant and record reasons in writing while issuing a warning or imposing costs on complaints which are devoid of merit. This will restore faith in complainants about the adjudication process being robust and fair.
23. Alternate Dispute Resolution			
23.	If the Board is of the opinion that any complaint may more appropriately be resolved by mediation or other process of dispute resolution, the Board may direct the concerned parties to attempt resolution of the dispute through mediation by a body or group of persons designated by the Board or such other process as the Board may consider fit.	If the Board is of the opinion that any complaint may more appropriately be resolved by mediation or other process of dispute resolution, the Board may direct the concerned parties to attempt resolution of the dispute through mediation by a body or group of persons **such as civil society or consumer organisations** designated by the Board or such other process as the Board may consider fit.	Civil society and consumer organisations with experience in promoting grievance redressal mechanisms like CUTS Grahak Sahayata Kendra[92] should be engaged to ensure that Alternate Dispute Resolution (ADR) mechanisms reach all consumers.
24. Voluntary Undertaking			
24 (4)	Where a person fails to comply with any term of the voluntary	Where a person fails to comply with any term of the voluntary undertaking	On the non-compliance of voluntary undertaking, while the Board can levy penalties as per Section 25 of the Bill,

[92] Consumer Care Centre (Grahak Sahayata Kendra) | CUTS Centre for Consumer Action, Research & Training (CART), *available at:* https://cuts-cart.org/consumer-care-centre-grahak-sahayta-kendra/

	undertaking accepted by the Board, the Board may, after giving such person, a reasonable opportunity of being heard, proceed in accordance with section 25 of this Act.	accepted by the Board, the Board may, after giving such person, a reasonable opportunity of being heard, proceed in accordance with section 25 of this Act **and issue specific performance orders, to persons involved, as may be required to ensure compliance with the provisions of the Act.**	the Board is not empowered to issue such orders to persons involved, as may be required to ensure compliance with the provisions of the Bill. Accordingly, the Board should be empowered to issue specific performance. It should be allowed to issue such orders to persons involved, as may be required to ensure compliance with the provisions of the Act.
25A. Data Protection Fund			
25A.	**Insertion of New Section - Data Protection Fund**	**A fund shall be constituted and called the Data Protection Fund, which shall be managed by the Board. It shall be made functional as per the following:** **(1) All sums realised by way of penalties by the Board under this Act shall be credited to the Data Protection Fund.** **(2) The Board shall utilise the Data Protection Fund solely for the purpose of carrying out the functions under subsection 20(5) of this Act.**	There is no mention in the draft Bill about where the funds raised from penalties under the Bill will be credited. It seems that the same is envisioned to be credited in the Consolidated Fund of India. For performing the functions laid down in the suggestion Clause 20(5), there is a need for the Board to have the adequate funds. On the lines of consumer welfare fund set up under the Central Excise and\ Salt Act,[93] the CGST Act 2015,[94] the Telecommunication Consumers Education and Protection Fund,[95] the draft Bill must also provide for the creation of such funds for purposes mentioned under the suggestion Clause 20(5). Accordingly, the draft Bill should provide for the creation of a Data Protection Fund which could specifically be

[93] Innovative Funding for Consumer Groups, Intergovernmental Group of Experts on Consumer Law and Policy, 2017
[94] See https://consumeraffairs.nic.in/organisation-and-units/division/consumer-welfare-fund/overview
[95] Telecommunication Consumer Education and Protection Fund Regulation, *available at* www.trai.gov.in/sites/default/files/201209030250489400257regulation15jun07%5B1%5D.pdf

		(3) The Board may, transfer a part of the sum remaining in the Data Protection Fund after carrying out functions under subsection 20(5) of this Act to the Consolidated Fund of India, after recording reasons in writing for doing so. **(4) The Board may also financially support independent civil society and consumer organisations to undertake research in the field of data protection and related areas, as per the subsection 20(5) of this Act.**	used for increasing users' knowledge regarding the mechanisms through which they can better exercise their rights under the draft Bill.[96] The penalties levied under this Bill may be huge and the collected sum may remain unutilised after performing the necessary activities for promoting awareness about data protection and other purposes as mentioned in subsection 20(5). Considering this, the Board may transfer such additional funds to the Consolidated Fund of India after recorded reasons in writing. This will also assist in making users more familiar to consent managers. For this, there should be a provision for funding experienced and credible civil society organisations to undertake user awareness generation and capacity building activities. Further, considering that consumer organisations are in a good position to take up the cause of aggrieved consumers and present their case, these funds may also be used to equip them with sufficient and sustained financial resources, in order to ensure that they perform this task of research and advocacy while meeting the appropriate standards.
Chapter 6: MISCELLANEOUS			
26. Power to make Rules			

[96] CUTS Submission to the Joint Committee on The Personal Data Protection Bill, 2019, *available at* https://cuts-ccier.org/pdf/submission-pdpb-2019.pdf

26. (1)	The Central Government may, by, notification make Rules consistent with the provisions of this Act to carry out the provisions of this Act.	The Central Government may, by notification make Rules consistent with the provisions of this Act to carry out the provisions of this Act. **While making Rules, the Central Government will adhere to the Rule making procedure mentioned in Section 3 of this Act.**	Under Clause 26(1), while making Rules, the Central Government should uphold the principles of transparency and do appropriate public consultation. Accordingly, it is recommended that the powers to make Rules should be accompanied by the Central Government following cost-benefit analysis and due public consultation in a transparent manner. The process to be followed for rule-making is suggested in Section 3 and the same should be followed here.
26. (2)	Every Rule made under the provisions of this Act shall be laid as soon as may be after it is made, before each House of the Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or both Houses agree that the rule should not be made, the rule shall thereafter have effect only in such modified form, or be of no effect, as the case may be; so, however, that any such	Every Rule made under the provisions of this Act**, along with views and suggestions for changes received from various stakeholders,** shall be laid as soon as may be after it is made, before each House of the Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or both Houses agree that the rule should not be made, the rule shall thereafter have effect only in such modified form, or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that	While the process defined in Clause 26(2) is necessary, it is not a sufficient measure to ensure checks and balances on the rule-making power of the Central Government. There is a need to incorporate the principles of accountability and transparency in this process. The Rules placed before Parliament should accompany key suggestions received from stakeholders and their suggested changes. This will enable the Parliament to understand the nuances of the subject matter and understand the views of different stakeholders while arriving at any decision.

	modification or annulment shall be without prejudice to the validity of anything previously done under that rule.	rule.	
27. Power of Central Government to amend Schedules			
27. (1)	The Central Government may, by notification, amend Schedule 1 to this Act. No such notification shall have the effect of increasing a penalty specified in Schedule 1 to more than double of what was specified in Schedule 1 when this Act was originally enacted.	The Central Government, **in consultation with the Board** may, by notification, amend Schedule 1 to this Act. No such notification shall have the effect of increasing a penalty specified in Schedule 1 to more than double of what was specified in Schedule 1 when this Act was originally enacted.	As the Board will be performing the adjudicatory function, it is necessary to consider its views on any change in the penalty amount. Accordingly, it is recommended that the change in the penalty amount under the Clause 27(1) is made in consultation with the Board.
28. Removal of difficulties			
28. (1)	If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, before expiry of five years from the date of commencement of this Act, by an order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to it to be necessary or expedient for removing the	If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, before expiry of five years from the date of commencement of this Act, by an order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to it to be necessary or expedient for removing the difficulty. **Such orders will be proportionate to the intended objectives, made in a**	Considering the growing and fast-changing pace of the digital economy, such a Clause may be necessary. However, the Clause only specifies that such an order made will not be inconsistent with the act and will be based on necessity. Such orders should also follow the principle of proportionality concerning removing the intended difficulty. Further, the removal process of difficulties should be transparent, and a cost-benefit analysis must be performed to ascertain that the order will achieve the intended objectives.

	difficulty.	**transparent manner and made after conducting cost-benefit analysis.**	
30. Amendments.			
30. (2)	Clause (j) of sub-section (1) of section 8 of the Right to Information Act, 2005 shall be amended in the following manner: (a) The words "the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information" shall be omitted; (b) The proviso shall be omitted.	**Withdraw.**	As per the Clause 30(2), personal information of public officials will be completely exempt from disclosure. The principle of upholding the privacy of public officials should not trump transparency as this may lead to them being non-accountable as required under the provisions of the Right to Information (RTI) Act. This effectively dilutes the RTI Act. Accordingly, Clause 30 (2) must be removed.

Consumer Unity & Trust Society (CUTS) expresses gratitude to MeitY for inviting comments and suggestions on the draft Digital Personal Data Protection Bill 2022. CUTS looks forward to MeitY accepting the above suggestions and assisting in its efforts to empower consumers and lead to effective and optimum regulation- making to protect personal data of the citizens. We would be glad to make an in-person presentation of our submission before MeitY.

For any clarifications/further details, please feel free to contact: Neelanjana Sharma (njs@cuts.org), Prince Gupta (prg@cuts.org), and Asheef Iqubbal (aql@cuts.org), Senior Research Associates at CUTS International. We are thankful for the support of Amol Kulkarni (amk@cuts.org).