Access Now's Submission on the Draft Digital Data Protection Bill, 2022 (MyGov Format)

PRELIMINARY	
TOPIC	**RECOMMENDATIONS (2500 characters each)**
Chapter as a Whole	The Bill excludes offline processing of personal data from its scope, meaning that the collection of all personal information offline would not, among others, require the consent of the data principal. Data principals can be subjected to harms from data processing *even in* offline formats (such as discrimination for filling an offline form mentioning their religion or caste or transgender status). Large businesses and even government offices carry out large-scale manual processing of personal data offline to this date. Forms such as the census form are also filled up to this date offline. The exclusion of collection of personal data offline in all these cases would result in excluding the most significant manner in which information is collected in India today. Similarly, employers collecting employee information at scale, as well as schools and colleges routinely collect sensitive forms of information to this date in offline form. Excluding the collection of such information from the scope of the Bill *entirely* without considering the *scale* at which manual processing is excluded appears to *over-exclude* manual processing of personal data even when it may not be desirable. Allowing offline processing to fall outside the scope would also create regulatory arbitrage, given the incentives for businesses to use paper-based mechanisms to collect data to evade data protection obligations, having undesirable policy consequences.

	At present, the consent requirement does not apply for publicly available information. If information initially shared offline without consent of the data principal is subsequently published in digital form, the Bill would deem consent of the user for such publication despite heightened privacy risks associated with such publication, an anomalous consequence of the scope considered with the deemed consent ground. ***Access Now recommends*** **easing the requirements of small players, by providing some exemptions to small entities processing personal data manually with strict limitations and principles. This could apply to some early-stage startups and small businesses such as Kirana stores rather than *entirely* excluding personal data processed offline from its scope.** ***Access Now recommends*** **that offline personal data should be included within the scope of the Bill to empower people to make informed decisions and enforce their rights in respect of personal data, with narrowly defined and clearly limited exclusions for small-scale offline processing.**
Short Title and Commencement	The Preamble in previous versions of the Bill, presupposed 'a relationship of trust' between persons and entities processing personal data, to protect the privacy of individuals relating to their personal data, and to create a framework of accountability for entities processing personal data. However, this language on trust between data fiduciaries and data principals is conspicuously absent from the preamble.

	Presupposing a relationship of trust between data fiduciaries and data principals, although not adequate in itself, was a progressive step towards creating a framework of accountability for data fiduciaries. It recognized the idea that irrespective of the consent of the data principal, data fiduciaries are bound by principles of accountability in the nature of fiduciary duties such as those of care and loyalty characteristic in these relationships. The term fiduciary has historically held significance under Indian law governing special responsibility of persons put in positions of trust (such as doctors). The Bill does however seem to create such a relationship through references to data collectors as 'data fiduciaries'. Defining entities controlling the processing of personal data as 'data fiduciaries' itself is not enough. Given that the preamble would play a considerable role in helping courts determine the overarching principles and objectives governing the Bill, we recommend further clarifying the relationship between data fiduciaries and data principals in the preamble of the Bill. ***Access Now recommends*** **the incorporation of express language on 'a relationship of trust' between data principals and data fiduciaries in the Preamble, to ensure heightened accountability for fiduciaries.**
Definitions	The Bill defines 'personal data' as 'data about an individual who is identifiable by or in relation to such data'.[1] The definition of personal data under the previous versions explicitly included data which directly *or indirectly* identifies an individual. This position was compatible with global best practices such as that under the General Data Protection Regulation (**GDPR**). In fact, in the previous version, the definition also

[1] Section 2(6), Digital Personal Data Protection Bill, 2022, available at https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf .

explicitly included *inferences* drawn from such data for the purpose of profiling', which was consistent with progressive practices such as that under the GDPR[2]. The present definition under the Bill however does not reference indirectly identifiable data and inferred data from the scope of personal data. Further, the Bill also deletes inferences drawn from an individual's personal data from the scope of personal data unlike the previous version, which should also constitute personal data, given the likelihood of such information also relating to an individual. The removal of this language from the explicit text of the Bill may lead to the inference that the legislative intent behind this deletion was to exclude these categories of information from the scope of the definition of personal data under the Bill. Even compared to the existing regime under the IT Act and the Rules, which covers information that is capable of directly or *indirectly* identifying an individual, the definition of personal information under the Bill is a much narrower definition which is not adequate to cover the manner in which individuals are typically identified given considerable advancement in the technological capabilities relating to algorithmic profiling.

Access Now recommends **reinstating the definition of personal data from the definition of DP Bill, 2021, such that even information that is *capable* of being identified, including indirectly or by inference, is included within the scope of the definition of personal data.**

The Bill considerably constricts the definition of 'harm', to exclude mental injury, identity theft, loss of reputation or humiliation, loss of employment, discriminatory treatment or blackmail, psychological

[2] Article 4(1). General Data Protection Regulation (**GDPR**), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

	manipulation and extortion. These categories of harm have been recommended by the Srikrishna Committee and the Joint Parliamentary Committee appointed by the Government. Harm can be in intangible form as well, in addition to being tangible (i.e. in terms of actual gain or loss). **Access Now recommends reinstating the wider definition of "harms" to cover the elements mentioned above into the text of the Draft Bill.**
Interpretations	**Treatment of Sensitive Personal Data** The previous versions of the Bill recognised sensitive personal data as a distinct category. Its definition included vulnerable categories of information (e.g. genetic information). These categories enjoyed special protection through *inter alia* the requirement to obtain 'explicit' consent to collect such information, allowing an elevated degree of protection in relation to such information. Access Now believes that non-compliance with data protection obligations in relation to these categories of information pose a considerably heightened risk to data principals. The Bill does away with the recognition of such categories as a distinct category warranting a greater degree of protection, with special duties. Further, the Data Protection Authority envisioned in the previous version of the Bill had the ability to specify through regulation *additional safeguards or restrictions* for the purposes of repeated, continuous or systematic collection of sensitive personal data for profiling of such personal data. However, the Bill does away with this requirement. While the removal of the category of critical personal data solely for the purpose of data localisation is a welcome move, the removal of special

	protection for specific categories of data posing a relatively higher risk to data principals is an unwelcome step. ***Access Now recommends*** **reintroducing the categorisation of specific categories of information as sensitive personal information and the associated heightened obligations from data fiduciaries.** **The processing of sensitive information should only be authorized if users have given free, informed and explicit consent, and in alignment with principles of necessity and proportionality, data minimisation and purpose limitation, and limited and defined data retention.**
Application of the Act	Although the Bill applies to persons residing outside India whose personal information is being processed in India, Section 18 of the Bill exempts personal data of data principals not within the territory in certain circumstances. This means that individuals residing outside India would not have any effective judicial remedy and legal recourse to a breach of their rights in India. Persons residing outside India should also be able to obtain effective remedy and seek legal recourse to hold data fiduciaries in India accountable for their data processing activities. In fact, the absence of this would affect the perception of adequacy of India's data protection regime by foreign authorities, such as in the European Union, and therefore adversely impact cross border data flows and trade agreements . ***Access Now recommends*** **extending the scope of the rights of data principals, and the obligations of data fiduciaries under the Bill to persons residing outside India as well and empowering such**

	individuals to obtain effective judicial remedy to enable smooth cross border data flows.

OBLIGATIONS OF DATA FIDUCIARY

TOPIC	RECOMMENDATIONS (2500 characters each)
Chapter as a Whole	The DP Bill 2019 required businesses to prohibit the processing of personal data except for specific, clear and lawful purposes. Further, every person processing personal data had to do so in a fair and reasonable manner, to ensure the privacy of data principals, and only for purposes consented to, in the context and circumstances in which data was collected.[3] However, even these limited requirements have been done away with in the Bill. In fact, the ability of data fiduciaries to process personal information in a manner that is not fair and reasonable is incompatible with the Indian Supreme Court's judgment in *KS Puttaswamy v Union of India* (**Privacy Judgment**)[4] which requires that intrusions into the fundamental right to privacy are fair, just, reasonable and proportionate.[5] It is essential to incorporate principles aligned with international best practices and rights frameworks, as well as the Privacy Judgment – these include the principles of necessity and proportionality, purpose limitation and data minimisation. ***Access Now recommends*** **incorporating essential principles for data protection, including principles of necessity and proportionality,**

[3] Section 5(a), The Personal Data Protection Bill, 2019, available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

[4] https://www.ssoar.info/ssoar/bitstream/handle/document/54766/ssoar-indrastraglobal-2017-11-bhandari_et_al-An_Analysis_of_Puttaswamy_The.pdf?sequence=1

[5] https://www.ssoar.info/ssoar/bitstream/handle/document/54766/ssoar-indrastraglobal-2017-11-bhandari_et_al-An_Analysis_of_Puttaswamy_The.pdf?sequence=1

	purpose limitation and data minimisation, in adherence with international best practices, human rights frameworks, and the Supreme Court's judgments
Grounds for Processing Personal Data	The previous versions of the Bill recognised 'sensitive personal data' as a distinct category of personal data, subject to special obligations. The definition of sensitive personal data included vulnerable categories of information such as genetic information and biometric information. These categories of information enjoyed special protection through *inter alia* the requirement to obtain 'explicit' consent prior to collecting such information, allowing an elevated degree of protection in relation to such information. Non-compliance with data protection obligations in relation to these categories of information pose a considerably heightened risk to data principals. The new draft should not do away with the recognition of such categories as distinct and special warranting a greater degree of protection, with heightened duties. For instance, the previous version of the Bill only allowed for processing personal data other than sensitive personal data, without consent of data principals pursuant to grounds such as recruitment or termination of employment or provision of to provide any service to, or benefit sought by, the data principal who is an employee of the data fiduciary. Further, the Data Protection Authority had the ability to specify through regulation *additional safeguards or restrictions* for the purposes of repeated, continuous or systematic collection of sensitive personal data for profiling of such personal data. **Remove Broad Legal Bases/Grounds for Processing Based on 'Deemed Consent'**

	The Bill makes the concept of consent meaningless by assuming it through an unprecedented concept of 'deemed consent', even when there is not any consent of the user. Even though grounds such as legitimate interests exist under the GDPR, they are narrowly tailored, intended to apply to specific instances and subject to specific guidelines contained within the GDPR. For example, recital 47 of the GDPR specifies that reliance on legitimate interests as a ground for processing personal data would require a *careful assessment* including of whether a data principal can *reasonably expect* at the time and context of collection of personal data whether the processing can take place. ***Access Now recommends*** **that public interest, and fair and reasonable processing should be removed as grounds for processing personal data, given that they are incompatible and overbroad exceptions that do not satisfy the necessity and proportionality test laid down through the Privacy Judgment. Further, there must be separate categorisation and associated heightened responsibilities for data fiduciaries in the context of processing of sensitive personal data.**
Notice	The Bill removes prescriptive requirements that previously made data fiduciary obligations relatively clear and predictable for compliance and enforcement. For instance, the detailed specifications of what needs to be included in a privacy notice has been removed. However, in the absence of these prescriptive requirements, businesses may not predictably know what degree of specification in their privacy notice would comply with this requirement. Similarly, the requirement to notify data breaches previously also specified the need to mention the nature of personal data, the number

	of data principals, and the possible consequences of the breach and mitigating actions taken towards remedying the breach, which have been deleted from the Bill. Further, the previous version also required significant data fiduciaries to maintain a record of processing activities in such form and manner as specified through regulation. This included important operations in the life-cycle, periodic review of security standards or other matters specified. The previous version also imposed prescriptive requirements relating to the functions of the data auditor, specifying that they would be responsible for evaluating the compliance of the data fiduciary, through clarity and effectiveness of notices, effectiveness of measures adopted, transparency in relation to processing activities, security safeguards adopted and responses to personal data breaches. However, these requirements have also been removed from the Bill without any compelling reason. These obligations were fair and reasonable and not onerous on platforms, given the very definition of significant data fiduciary assumes the characterisation of platforms that have a large volume of users. ***Access Now recommends*** **reintroducing the prescriptive requirements in the Bill that were explicit in the previous versions for clarity and predictability for companies as well as persons whose data is involved.**
Consent	At present, the Bill allows data principals to give their consent through 'consent managers', a data fiduciary enabling a data principal to give,

	manage, review and withdraw their consent through an accessible, transparent and interoperable platform. There needs to be further clarity on the role and functioning of the consent manager. For instance, there is currently nothing to ensure that the consent manager acts in the best interests of the data principal. There is also no requirement that the consent manager is structurally and functionally *independent* of the data fiduciary that is controlling the processing of personal data of a data principal in a given context. Unlike account aggregators envisioned by regulation created by the Reserve Bank of India, there is also no requirement under the Bill that consent managers refrain from engaging in any business other than consent management. Given that consent itself would practically not be exercised freely in many situations, the transfer of the right to exercise the fundamental right such as privacy is incompatible with the Indian Constitution and unprecedented. ***Access Now recommends*** **that a detailed explanation on the role, independence, and functioning of a consent manager be incorporated in the draft bill, with provisions to ensure transparency, accountability, and redress, in a way that ensures primacy of the data principal's right to privacy**.
Deemed consent	The conceptualisation of deemed consent significantly undermines the value of consent as it allows consent to be deemed in overbroad, vague and undesirable situations, such as in case of 'any public interest in processing'. This tilts the scale dramatically in favour of data fiduciaries and against data principals. ***Access Now recommends*** **considerably reducing the scope of the grounds on which consent can be deemed to exist and considered**

	valid, in accordance with strict standards of necessity and proportionality. In a situation where consent would not be a free choice, including if required to be able to access public or private services, such consent cannot be considered lawful.
General Obligations of Data Fiduciary	The Bill does not create a meaningful framework of accountability beyond terming (by way of nomenclature) entities determining the means and purposes of processing personal data as "data fiduciaries". It is not sufficient to use the terminology to indicate a fiduciary relationship between the data fiduciary and the data principal; the fiduciary obligations should be set out in the legislation. The Bill does not require data fiduciaries to adequately discharge a duty of loyalty towards data principals and their right to privacy; to ensure the best interests of the data principal, with a general duty to prevent harm. While there is a requirement to process personal data of children in a manner that does not cause harm, there is no similar requirement for other data principals. ***Access Now recommends*** **specifying the nature and precise scope of the fiduciary obligations of data fiduciaries to data principals within the scope of the Bill. This should include the obligation to ensure that in a conflict of interest between the interests of the data fiduciary and that of the data principal with regard to the personal data of the data principal, the data principal's interests would prevail.** ***Access Now recommends*** **the inclusion of a general duty of care on the part of data fiduciaries to prevent harm to data principals.**

Additional obligations of significant data fiduciaries	The DP Bill, 2021 required significant data fiduciaries (SDFs) to maintain an accurate and up-to-date record of their processing activities. This also required significant data fiduciaries to carry out periodic review of security safeguards and data protection impact assessments. It is important for SDFs to maintain records of their processing activities for regulators to be able to oversee the implementation of the Bill, and whether SDFs are complying with their data protection obligations under law. Further, the assessment process for categorisation of a data fiduciary as a significant data fiduciary should be clearly set out in the bill. **Access Now: We recommend that explicit accountability requirements for SDFs, including to maintain records of their processing activities, review security safeguards and conduct detailed data protection impact assessments, be incorporated. Further, the assessment process for categorisation of a data fiduciary as a significant data fiduciary should be clearly set out in the bill.**

RIGHTS AND DUTIES OF DATA PRINCIPAL	
TOPIC	**RECOMMENDATIONS (2500 characters each)**
Chapter as a whole	The current draft removes the provision conferring on data principals the right to seek compensation for harm caused as a consequence of non-compliance with the data protection legislation. Notably, previously, this provision allowed for an uncapped compensation to data principals. In fact, even Section 43A of the Information Technology Act, 2000 allows individuals uncapped compensation if a body corporate

	is negligent in implementing and maintaining reasonable security standards. The removal of the right to compensation would be a regressive step. The ability to seek compensation is an important feature of any data protection law, without which the individual would not be able to seek effective judicial redress. Crucially, the ability of individuals to avail effective judicial redress is also a factor considered by the EU for European businesses outsourcing data to India, in assessing whether Indian law provides an "adequate" level of protection to individuals residing in the EU. Since individuals may not be able to seek recourse against the state for breaches to the fundamental right to privacy, compensation enables individuals to avail judicial remedy through pecuniary remedy in the nature of compensation. In the absence of the incentive to be compensated, individuals would not have the incentive to pursue legal action and incur financial and opportunity costs to file complaints against data fiduciaries. Compensation forms part of most data protection regimes across the globe. We believe that penalty provisions are not adequate to compensate or redress financial or other types of suffering such as exclusion or discrimination caused to an individual as a consequence of a failure of a data fiduciary to comply with data protection law. ***Access Now recommends*** **reintroducing the right of individuals to seek compensation under the Bill**.
Right to information about personal data	The Bill deletes the requirement that businesses be transparent about the manner of their use of algorithms. This requirement was introduced by the Joint Parliamentary Committee constituted by the Government of India in a welcome step towards increasing algorithmic transparency.

At present, the use of opaque algorithms to make decisions that impact individuals can result in significant harm, such as the ability of individuals to access essential goods or services. Transparency in decision-making helps in creating a sense of accountability to citizens at large, which in turn helps in building trust by individuals in systems that rely on algorithms. Transparency in the manner of decision-making also makes consent of individuals more meaningful. Under the GDPR, for instance, the GDPR allows individuals with the right to know about the existence of automated decision-making including profiling, as well as the right to receive meaningful information about the logic involved and the significance and the consequences of processing on the individual.

Further, the right to information under the new draft does not go far enough. Under the right to information about personal data, the Data Principal can only obtain a "summary" of the personal data of the Data Principal being processed by the Data Fiduciary – not the full scope and substance of personal data.

Access Now recommends **introducing a right to explanation in the text of the Bill for a data principal to receive meaningful information about the manner in which decisions are made by a data fiduciary on the basis of the personal information of a data principal, through automated as well as non-automated means, and to enable algorithmic transparency. Further, a data principal should have the right to obtain the full scope and substance of their personal data being processed by a data fiduciary, not only a summary.**

Right to correction and erasure of personal data	**Removal of the Right to Data Portability** The Bill has removed the right to data portability from its text, unlike the previous versions. The right to data portability is essential towards ensuring individuals have the ability to move across platforms seamlessly without worrying about being able to move their data from one platform to another and losing their existing data. The right to data portability helps in preventing businesses from adopting exploitative data practices through the enjoyment of market power, by creating walled gardens that individuals are not able to migrate out of to better platforms. For example, if a user wants to move from WhatsApp to another messaging platform, if WhatsApp is not required to enable this migration and provide the data in a machine readable format, the user would remain entrenched/stuck in the platform without being able to migrate to more competitive options. The right to data portability is an important feature of the right to privacy since it enables individuals to exercise their autonomy in the digital economy. ***Access Now recommends*** **reintroducing the right to data portability within the text of the Bill.**
Right to grievance redressal	A robust grievance redressal mechanism is crucial for an effective data protection regime. The current provision fails to establish such a mechanism, and contains ambiguous language such as "as may be prescribed", allowing excessive leeway to the government, and creating scope for arbitrariness and misuse. ***Access Now recommends*** **establishing a robust grievance redressal mechanism, for effective enforcement of rights, in the legislation,**

	and to refrain from allowing for such essential provisions to be prescribed through rule-making and delegated legislation.
Right to nominate	Under the GDPR, individuals have a right to appoint a non-profit organization active in the field of data protection to act on behalf of data principals when complaining to the regulator or making a complaint to the court. However, the right envisioned in the current draft only refers to the ability of another individual to exercise a data principal's rights in the event of death or incapacity of the data principal . ***Access Now recommends*** **that the right to nominate under the current draft be amended to also include the right to appoint a non-profit organization to act on behalf of data principals in proceedings before the regulator or court. This will enable greater access to redress and remedy.**
Duties of Data Principal	**Removal of Duties on the Data Principal** The Bill requires data principals to incur a cost of ten thousand rupees for filing a "frivolous" complaint. The draft does not define "frivolous" or set out the factors to be considered when making this assessment. This adds to the uncertainty and lack of predictability surrounding the Bill. International best practices on data protection do not impose the burden on the individual but instead on companies under data protection law. The possibility of a complaint being perceived as frivolous and a data subject having to pay a penalty of ten thousand rupees would discourage individuals from filing complaints, particularly since the right to compensation under PDP Bill 2019 has been problematically done away with. In fact, even under the Information

	Technology Act, 2000 read with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (**Privacy Rules**), section 45 entitles users to compensation to each person affected by a non-compliance with a provision under the rules, where there is no specified penalty. Removing the compensation provision would be a regressive step even when compared to the law at present. ***Access Now recommends*** **reintroducing the right to compensation for data principals as under the previous versions of the Bill.**

SPECIAL PROVISIONS

TOPIC	RECOMMENDATIONS (2500 characters each)
Chapter as a Whole	India has recently committed to the Joint Declaration on privacy and the protection of personal data.[6] This commitment requires that India adopt (i) a comprehensive legal framework for data protection that applies not only to the private sector, but also the public sector (i.e. the state) (ii) internalise core principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, limited data retention, data security and accountability under all circumstances (iii) a framework which enables individuals to exercise and enforce their rights (iv) safeguards for international data transfers (such as the protection of personal data of foreign citizens in India) (v) a framework for independence oversight by a dedicated supervisory authority. Trust works on the basis of reciprocity, and as India expects trusted geographies to fulfill these commitments prior to enabling data transfers to them, it is also

[6] https://www.eeas.europa.eu/eeas/joint-declaration-privacy-and-protection-personal-data_en

	necessary for Indian data protection law to achieve a standard of protection which fosters trust between India and other nations. Such trust can greatly encourage other countries to rely even more on India's outsourced Information Technology (**IT**) services. Similarly, as data principals are expected to trust data fiduciaries with their data, their right to privacy should be meaningfully protected with avenues for effective remedies, and the obligations of fiduciaries, in the private as well as public sectors, should be clearly set out to ensure accountability and transparency.Towards building this trust, **India needs to strive towards tangibly fulfilling the aforementioned commitments in the Joint Declaration**.
Transfer of Personal Data Outside India	The Bill has removed the requirement that personal data only be transferred to third countries that maintain the same or adequate level of protection as under Indian law. Instead, the Bill proposes a trust-based mechanism for data transfers. While the removal of onerous data localisation obligations *inter alia* relating to critical personal data are welcome, this provision that suggests the creation of a list of select jurisdictions still suffers from lack of clarity. ***Access Now recommends*** **that in order to truly enable business certainty and protection of rights, the bill, and not rules framed under it in the future, contain clear guidance on how the data protection frameworks in foreign jurisdictions are assessed for transfers, who makes the assessment, the independence of the authority doing so, and the ability of affected parties to challenge the decision.**

Exemptions	The Bill grants excessive discretionary powers to the Central Government to exempt government as well as private entities from the scope of the Bill. There is a complete lack of any meaningful safeguards and limitations, including the absence of any requirement to adhere with the standard of necessity and proportionality, as required under the Privacy Judgment – this dilutes the effectiveness of the entire Bill. The ability of the Government to exempt itself from the scope of the Bill without any independent or judicial oversight, leaves ample scope for misuse and arbitrary decision-making, to the detriment of people's rights. The government is a significant data fiduciary processing enormous amounts of personal data of citizens, and it cannot be granted unchecked powers as all the versions of the Bill so far have sought to do. Further, there ought not to be a blanket power to exempt any private entity from having to comply with the provisions of the Bill. ***Access Now recommends*** **the reduction of risk of mass surveillance and other privacy harms by establishing meaningful limitations and independent oversight mechanisms in relation to the power of the central government to grant exemptions under the Bill.** **The scope of exempting entities from the scope of the Bill should be narrowly tailored, permissible only when necessary and proportionate to achieve a narrow, prescribed purpose, and limited in time. The exemptions should not be extended to the requirement to respect fundamental principles of data protection such as fairness, lawfulness, purpose limitation, data minimization, transparency regarding the nature of exemption granted in a given**

	context, as well as the principle of accountability, to ensure the disincentive of overbroad exemptions from being granted. **Further, the ability of the government to grant exemptions to private entities must be eliminated, or if necessary for small enterprises, the scope and circumstances must be clearly explained and limited.**

COMPLIANCE FRAMEWORK	
TOPIC	**RECOMMENDATIONS (2500 characters each)**
Data Protection Board of India	An independent regulatory authority is a cornerstone of an effective data protection regime. However, despite widespread criticism over the many drafts of the Bill, the Data Protection Board of India (DPBI) continues to lack independence from the government. The Government of India itself would be a significant data fiduciary, and therefore potentially a frequent party before the DPBI. Complete independence of the DPBI in all aspects, including appointment of its members and chairperson, and functioning, is non-negotiable. At present, the strength and composition including the appointment of members as well as the chairperson, structure, funding, and functions, are to be prescribed by the Central Government. This means that the Central Government would effectively have the ability to entirely control the structure and functions of the DPBI. Merely describing the DPBI as an "independent body" is not sufficient. Such independence must be reflected in substantive provisions pertaining to its structure and functions. ***Access Now recommends*** **introducing substantial modifications ensuring that the DPBI has meaningful, complete and absolute**

	autonomy and independence in all aspects, including its structure, composition, functions, policy-framing and decision-making processes.
Functions of the Board	Unlike the previous version of the Bill, the only specified functions of the Board are that of enforcement rather than that of a regulator, such that it is only required to determine non-compliance with the provisions of the proposed data protection law, direct data fiduciaries to take appropriate action urgently in response to a data breach, or modify, suspend or cancel its own decisions. The provision on the DPBI's functions lacks detail, and contains an ambiguous provision allowing the government to assign functions to the DPBI. The Data Protection Authority under previous versions of the bill was similarly lacking in terms of independence, but it had greater regulatory functions which are essential, including to monitor the application of the provisions of the law, maintain a database of websites containing significant data fiduciaries and their trust scores, examine data audit reports, issue certifications of registration to data auditors, classify data fiduciaries and specify codes of practice. The ability to specify codes of practice was crucial to promote good practices of data protection and to create a culture of respect for data protection in India. ***Access Now recommends*** **that the DPBI's functions be set out in detail, and the government's power to assign functions and therefore determine its scope of enforcement be clearly defined and limited with safeguards. The DPBI must also be granted powers to regulate such as monitoring the application of the provisions of the law, maintaining a database of websites containing significant data fiduciaries and their trust scores, examining data audit reports,**

	issuing certifications of registration to data auditors, classifying data fiduciaries and specifying codes of practice,, while also explicitly recognising the DPBI's role as an oversight body, including over the government and public sector as a data fiduciary.
Review and Appeal	Unlike the previous version, the Bill does away with the appellate authority for the purpose of hearing appeals, and requires that appeals from decisions of the Board only lie to existing High Courts. However, given the sheer volume of internet users in India, and the potential number of complaints which may be raised before the board, it is likely that there may be a significant number of cases that would result in an appeal from the decision of the Board. An appeal to the High Court instead of an appellate authority is likely to increase the existing burden of discharging cases on these courts and result in significant delays. Additionally, the Bill currently appears to have a typographical or drafting error, as it says n appeal against any order of the Board shall lie "to the High Court", without indicating which High Court this would be - not is a provision creating indicating that will be subject to later notification. ***Access Now recommends*** **that an appellate authority which is structurally and functionally independent from the Government should be responsible to hear appeals from decisions made by the DPBI**. **The Government should also clarify which high court the current language is directed to.**
Alternate Dispute Resolution	Given acute information and power asymmetries between individuals and most data fiduciaries in the private and public sectors, alternate dispute resolution would not be suitable. If typically, enforcement of

	penalties requires individuals / users to incur considerable costs, they may be compelled to accept a direction to opt for alternate dispute resolution, which may ultimately not result in meaningful redress for individuals. Researchers suggest that less formal or transparent adjudicatory processes can increase inequality of bargaining power in alternate dispute resolution mechanisms.[7] ***Access Now recommends*** **removal of the provision empowering the DPBI to refer parties to alternate dispute resolution.**
Voluntary Undertaking	The ability of the DPBI to allow businesses to enter into voluntary undertakings undermines the seriousness of breaches of the fundamental right to privacy, and disadvantages data principals who are in most cases on the unfavourable side of the information and power imbalance as compared to private and public data fiduciaries. While admission of non-compliance and rectification of lapses are desirable, allowing voluntary undertakings even in cases involving serious non-compliance relegates the significance of the fundamental right to privacy. Serious non-compliances such as the failure to implement reasonable security safeguards, or failure to obtain consent appropriately or the failure to protect individuals' rights cannot be addressed merely by voluntary undertakings and more effective remedy is necessary, even to serve as a deterrent in the future. Even if the concept is to be retained, voluntary undertakings should suffice only in narrowly defined and limited situations – The data protection law in Singapore which perhaps this concept has been taken

[7]https://www.cambridge.org/core/journals/law-and-social-inquiry/article/abs/imbalances-of-power-in-adr-the-impact-of-representation-and-dispute-resolution-method-on-case-outcomes/B02FFE84EA2FE5F961A90907BF82F794

	from only permits the Commission to allow voluntary undertakings in case of specific non-compliances. Further, the affected parties/data principals should have the ability to provide inputs, the DPBI should have the power to require substantive modifications, and they should not place a blanket bar on proceedings under the law. ***Access Now recommends*** **eliminating voluntary undertakings as it would not sufficiently safeguard rights, and would further intensify the information and power imbalance between data principals and fiduciaries. In the event that they are to be retained, they must be permitted only for minor, clearly defined and limited non-compliances matters and must not place a blanket bar on pursuing proceedings. Further, affected parties must have the right to appeal or modify such undertakings and the DPBI must have the power to make substantive modifications to the undertakings.**
Financial Penalty	At present, the financial penalties do not have a requirement to incur a minimum fine under any circumstance, and the ceiling is pegged at specific amounts as opposed to a percentage of the specific data fiduciary's annual revenues/turnover. The absence of a minimum penalty, coupled with amount-specific ceilings may result in exceptionally high penalties for small and medium enterprises; and for large companies, it may result in penalties that make no dent in the resources at their disposal. Percentage based penalties would be more effective deterrents and would serve to disincentivise companies from breaching obligations – in alignment with international best practices. . ***Access Now recommends*** **incorporation of penalties based on a percentage of the data fiduciary's annual revenue/turnover, and**

	prescription of a minimum fine. Additionally, when considering a fine level, the regulators must consider if the proceeding concerns repeated offenses and/or offenders to be able to propose incremental and deterrent fines.

MISCELLANEOUS

TOPIC	RECOMMENDATIONS (2500 characters each)
Chapter as a whole	In an attempt to simplify the implementation of the data protection framework, the bill sacrifices much of the necessary nuance that was partially present in previous versions of the bill, and recommended by several stakeholders over many years. We appreciate the need to balance innovation and growth of early-stage startups on the one hand, with the need to protect people from considerable harm as a consequence of violations of their right to privacy on the other. Towards achieving this balance, the Bill relaxes many of the obligations contained in the previous versions, considering the nascent stage of data protection in India.[8] However, Access Now believes that the Bill needs to narrowly tailor these exemptions only for smaller businesses/early-stage startups, in a time-bound manner, instead of of all private and public data fiduciaries which have the infrastructural and financial capacities, and duty, to comply with nuanced data protection obligations imperative to protect the people's interests and rights.
Power to Make Rules	The scope for rule-making by government and delegated legislation is so wide that it could be used to change the core of the legislation itself. This undermines clarity and predictability, people's rights, business certainty, as well as the prospect of smooth cross border data flows. Strict limitations need to be incorporated in this regard, and substantive provisions, including for instance those pertaining to the grievance

[8]https://asia.nikkei.com/Spotlight/Comment/India-s-new-data-protection-bill-gets-Big-Tech-startup-support

redressal mechanism, functioning of the DPBI should be set out in the primary legislation, and not reserved for rules and delegated legislation.

Excessive powers for the Government to prescribe rules could result in over-delegation of powers to the executive, incompatible with the Indian Constitution. The Supreme Court has held that laws permitting overbroad or excessive delegation can be struck down for being vague and unconstitutional. The Bill enables the Central Government to prescribe or notify substantive provisions, including the following, on vague and overbroad grounds:

1. Exempt government agencies (for national security reasons or to prevent the incitement to any cognizable offense)
2. Exempt private data fiduciaries based on the volume and nature of personal data processed as well as for research, archival or statistical purposes) from the scope of the Bill
3. Technical, operational, financial and other conditions of consent managers
4. Fair and reasonable grounds for processing personal data
5. Form and manner of notifying the Board about a data breach
6. The types of processing of personal data that are likely to cause harm to a child
7. The obligations that need to be complied with by the significant dat fiduciary
8. The composition of the Board and the terms of appointment and service.

Further, the government also has the power to make prescriptions on several issues including notices, and to unilaterally amend the penalty

	schedule. ***<u>Access Now recommends</u>*** **strictly limiting the government's rule-making powers and scope for delegated legislation. Substantive provisions impacting the scope, scheme and implementation of the law, and people's rights, must be set out in the primary legislation with parliamentary scrutiny.**
Consistency with Other Laws	The previous version of the Bill clearly specified that data protection law would have an overriding effect notwithstanding anything inconsistent with any other law for the time being in force. Given the fact that the right to privacy is a fundamental right, if there are competing obligations of data fiduciaries under data protection law as well as other statutes, the obligation under data protection law should take precedence. Yet, at present, the Bill provides that the provisions of the Bill should be construed in addition to, and not construed in derogation of the provisions of any other law, and shall be construed as consistent with such law, for the time being in force. In the event of any conflict between a provision of the Bill and a provision of any other law for the time being in force, the provision of this Act shall prevail to the extent of such conflict. This language introduced in this version of the Bill compared to the deleted language is far more reconciliatory in nature, falling sort of recognizing the considerably high status enjoyed by obligations relating to privacy as a fundamental right under the Indian Constitution as compared to other legal obligations. As we note in our other feedback, this should be subject to ensuring that is does not undermine the Right to Information, as provided for under the Constitution and the regime created by the RTI Act.

	<u>Access Now recommends</u> incorporating language explicitly providing for the overriding effect of the data protection law to protect people's privacy. The data protection law should not override the RTI Act without further detailed study and consensus with stakeholders involved in RTI and government transparency.
Amendments	The Bill recommends the deletion of the following language from the Right to Information Act, 2005: "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". Access Now believes that transparency in governance is crucial for accountability and public trust. The above language is imperative to ensure that the right to information is carefully balanced with privacy. The deletion of the exception existing under right to information law above ensures the requirement to balance the freedom of speech and expression with the right to privacy, and prioritises compelling public interest vis-a-vis public records. However, the removal of the public interest exception would be detrimental to access to information by the public. In the absence of such language, it is possible that public servants would operate without any transparency in the manner of their functioning. Without a narrowly tailored public interest exception, it is likely that bureaucrats, judges and politicians would operate without transparency in their public functions, undermining accountability. **<u>Access Now recommends</u> consulting with stakeholders to carefully balance the right to information with the right to privacy, and**

narrowly tailor the public interest exception by incorporating the principle of necessity and proportionality, rather than removing it.

Schedule I

TOPIC	RECOMMENDATIONS (2500 characters each)
Any other feedback	The Bill does away with the concept of data trust scores, which were beneficial in creating a trust-based incentive for businesses to comply with data protection law. A data trust score enables individuals to have greater visibility over which data fiduciaries have better privacy practices, enabling privacy to be a consideration in individuals making meaningful choices in digital markets. In the absence of any reason for removing this requirement, Access Now recommends reintroducing trust-based data scoring. The Data Protection Bill, 2021 imposed criminal penalty for the intentional reidentification of an individual's anonymised personal information. This provision has been done away with in the current draft of the Bill. We would recommend reintroducing this provision. The possibility of reidentifying an individual from anonymised personal data poses the risk of data protection law not applying to a data fiduciary which decides to re identify an individual from anonymised personal data, defeating the purpose of excluding anonymised personal data from the scope of the Bill, given the potential privacy risk of re-identification.

Access Now recommends **the reintroduction of provision imposing a penalty for reidentification of data principal from anonymised personal data**.