Digital Personal Data Protection Bill 2022 - FOSS United Submission

On behalf of FOSS United, we would like to submit our comments on the Draft Personal Data Protection Bill 2022. FOSS United is an Indian non-profit focused on growing the Indian Free and Open Source Software (FOSS) ecosystem.

We appreciate the simple, non-legalistic language used in drafting the DPDP and the use of the pronoun “her,” which makes for a refreshing departure from the past. We also appreciate the use of examples to communicate the meaning of clauses.

We want to submit the following points for your consideration:

| **No** | **Current Text** | **Suggested Modification (if any)** | **Comment** |
| --- | --- | --- | --- |
| 1 | The DPDP Bill and the accompanying Explanatory Note do not make a reference to privacy even once! | Does the government plan to introduce a separate privacy bill, or is this bill supposed to serve as the privacy bill? If it is the former, we suggest that the bill be reworked with individual privacy at the heart of it. If not, we suggest a detailed explanation of what the government plans to do to protect privacy. | Data protection is merely the *means to an end*, which is the protection of the privacy of individuals. If the intention is to create a separate privacy bill, that should be mentioned in the explanatory note so that citizens have clarity on the same. |
| 2 | The title of the bill is “The Digital Personal Data Protection Bill, 2022.” This leaves open the question of how non-digital personal data will be protected. For example, NGOs working in rural areas have reported that when women recharge their mobile phone talk plans, shopkeepers providing the recharge often write down the phone numbers and sell them to others for as little as Rs 50. This is a (non-digital) violation of the fundamental right of privacy, and one wonders how such violations will be handled. | We suggest that the explanatory notes be made more detailed, and a section added on how the government plans to tackle privacy violations that are non-digital. | If privacy is a fundamental right, its violations -- digital and non digital -- have to be penalized. As citizens, we await clarity from the government on how it plans to do that. |
| 3 | Section 3(2) says “the option to access ... in English or any language specified in the Eighth Schedule to the Constitution of India” shall mean that the Data Principal may select either English or any one of the languages specified in the Eighth Schedule to the Constitution of India; |  | We welcome this clause because barely 10 percent of India’s population is English literate. This will help the vast majority of India’s population that can read Indian languages. We hope that the Data Protection Board will take this further by encouraging the creation of voice notices and other innovations especially designed for those Indians who are illiterate and cannot decipher written text. |
| 4 | Section 6 says, “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 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.” |  | Retrospective applications of a law should be avoided unless there are truly exceptional circumstances. |
| 5 | Section 7(4) says, “Where consent given by the Data Principal is the basis of processing of personal data, the Data Principal shall have the right to withdraw her consent at any time. The consequences of such withdrawal shall be borne by such Data Principal. The withdrawal of consent shall not affect the lawfulness of processing of the personal data based on consent before its withdrawal. The ease of such withdrawal shall be comparable to the ease with which consent may be given.” |  | We welcome this clause as withdrawing consent is often much more difficult than providing consent. We have seen cases where despite individuals opting out of an insurance scheme, they are endlessly harassed with calls to renew the same. If enforced well, this clause will put an end to such harassment. |
| 6. | Section 9 on General obligations of a data fiduciary | A fiduciary relationship is one where the service provider is expected to hold information in confidence or trust and act in the best interests of the information provider. As first principles, it would be good to clarify this explicitly in the Bill with explanatory notes so that fiduciaries have greater clarity on what they can and cannot do. For example, it is observed that when two people are using a ride hailing app to go to the same home location, the person who has set her location as “Home” is charged a higher fare as compared to the person who has not done so. This is a clear case of the information being provided by the Data Principal being exploited by the Data Fiduciary to extract a higher fare.  Since data fiduciaries are known to use data provided to them for purposes beyond the original scope, an example on purpose limitation could also be added. For example, social media companies collect a user’s mobile phone numbers for SMS Two Factor Authentication (2FA). While users share their data for security purposes, social media companies use it for marketing and data mining, which is beyond what users have consented to. | Examples on obligations of a data fiduciary and on purpose limitation to be added. |
| 6 | Section 18(2)(a) says that, “  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 | We recommend that the section on surveillance in the 2019 bill be restored. The 2019 Bill explicitly defined surveillance as a harm under Section 3(20), *“(ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled;*  *(x) any observation or surveillance that is not reasonably expected by the data principal.”*  We also recommend that Section 50 from the 2018 Bill on “Composition and qualifications for appointment of members,” be reinstated. The section reads:   (1) The Authority shall consist of a chairperson and six whole-time members.   (2) The chairperson and the members of the Authority shall be appointed by the Central   Government on the recommendation made by a selection committee consisting of—   (a) the Chief Justice of India or a judge of the Supreme Court of India nominated by the Chief Justice of India, who shall be the chairperson of the selection committee;   (b) the Cabinet Secretary; and   (c) one expert of repute as mentioned in sub-section (6), to be nominated by the Chief Justice of India or a judge of the Supreme Court of India nominated by the Chief Justice of India,in consultation with the Cabinet Secretary.   (3) The procedure to be followed by the selection committee for recommending the names under sub-section (2) shall be such as may be prescribed.  (4) The chairperson and the members of the Authority shall be persons of ability, integrity and standing, and must have specialised knowledge of, and not less than ten years professional experience in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, and related subjects.   (5) A vacancy caused to the office of the chairperson or any other member shall be filled up within a period of three months from the date on which such vacancy occurs.   (6) The Central Government shall maintain a list of at least five experts who have specialised knowledge of, and professional experience in the field of data protection, information technology, data management, data science, cyber and internet laws, and related subjects. | Section 18(2)(a) combined with the fact that the Data Protection Board will be appointed by the Central Government gives the government overriding powers that are not in keeping with the checks and balances that are an integral part of democracy. The state is the largest Data Fiduciary in the country, and a Board that is appointed by (and beholden to) the state, cannot be expected to provide any reasonable oversight on the state’s functioning as a Data Fiduciary.  Fundamental rights are rights that cannot be alienated from the individual except under narrowly prescribed conditions. Fundamental rights are also meant to protect individuals against arbitrary state action, because the state wields tremendous power through its control of coercive instruments like the police, tax authorities and its ability to surveil citizens. Privacy as a fundamental right means that a citizen's right to privacy is supreme and even the state cannot impinge on it. A privacy (or even a data protection) bill that does not prescribe guardrails against state action is as one-sided as the End User License Agreements (EULA) that users accept when they sign up to most Internet platforms. The balance of power must therefore be restored in favor of citizens in this bill by narrowing the exceptions in this Bill and prescribing guardrails to the exercise of state power. |
| 7 | Section 21(1) says that, “The Board shall function as an independent body and, as far as possible, function as a digital office and employ such techno-legal measures as may be prescribed.” | We also recommend that Section 50 from the 2018 Bill on “Composition and qualifications for appointment of members,” be reinstated. Since (A) the Data Protection Board is expected to function like a Civil Court, and (B) is an institution of national importance, and (C) it is expected to provide oversight over ALL data fiduciaries, it is only appropriate that the Chief Justice of India or their nominee be a part of the selection committee. Given the specialized knowledge required for data protection, subsections 4 and 6 are also essential. | As citizens, we would like to understand *how* the independence of this critical institution will be assured and this must be enshrined in the bill itself. |