

# The Digital Personal Data Protection Bill, 2023

The Bill grants the Central Government excessive discretionary power, does not create an independent regulator, creates uncertainties in cross-border data flows, and undermines people's rights. It must be significantly improved by Members of Parliament in consultation with stakeholders in order to truly be an acceptable law, let alone a world class data protection act.

## **No Independent Regulator**

- The strength, composition, and terms and conditions of service of the Data Protection Board of India (DPBI) and its members will be prescribed by the Central Government.
- The government is a significant data fiduciary, and will be a frequent party before the DPBI.
- The bill must include substantive provisions on the structure and functioning of the DPBI to ensure it has meaningful independence in its operations and decision-making. **(Chapter V)**

## **Exemptions legitimise surveillance**

- Government can exempt itself and other entities from obligations under the bill, without any public or judicial oversight, creating risks of mass surveillance and serious privacy harms.
- Exemptions should be narrowly tailored, permissible only when necessary and proportionate to achieve a narrow, prescribed purpose, and limited in time.
- In the private as well as non-profit sector, exemptions should only be granted to small enterprises, with the scope and circumstances being clear and limited. **(Section 17)**

## **Appeals to the Telecom Disputes Settlement and Appellate Tribunal, and not High Courts, violates rights**

- The TDSAT lacks the authority to adjudicate disputes pertaining to the fundamental right to privacy and personal data. The High Courts' writ jurisdiction must be available for effective remedy.
- The TDSAT has only one bench in New Delhi which does not enable easy access to appeal for Data Principals across the country. **(Section 29, 30)**

## **'Certain legitimate uses' are overbroad and fail to keep consent necessary and meaningful**

- The bill must restrict the processing of personal data without consent. Permitting any State or private entity to process data for other than specified purposes places the burden on the Data Principal to "opt out" of processing for other purposes, instead of enabling her to "opt in".
- These exemptions are incompatible with the necessity and proportionality test laid down by the Supreme Court in its Privacy Judgment.
- "Previously" given consent cannot be used in a perpetual manner and/or for other purposes. **(Section 7)**

## **Need for clarity and checks on cross-border data transfer restrictions**

- For business certainty and the protection of rights, restrictions should be imposed with approval of the DPBI and public consultation. **(Section 16)**

### **Weakened Rights**

- For eg., the right to information, and compensation: The bill overrides the Right to Information Act, diminishing government accountability; and removes the right to compensation while imposing costs on individuals for “frivolous complaints”. *(Section 15, 28, 44)*

### **Unchecked government powers to obtain and block information**

- The Central Government can “call for” information from the Board, any Data Fiduciary, or any “intermediary” under the IT Act on unspecified grounds. The lack of limitations and safeguards is incompatible with the right to privacy.
- The Central Government and the Board can block access to data in “the interests of the general public” if two or more monetary penalties have been imposed on the Data Fiduciary. This is a vague and overbroad ground for censorship of online data not falling under Article 19(2) of the Constitution. It also risks enhancing the existing excessive and opaque powers of the government under Section 69A of the IT Act. *(Section 36, 37)*