

# HOW DIFFERENT IS THE NEW DATA PROTECTION BILL?

Relevant for: Science & Technology | Topic: IT, Internet and Communications

To enjoy additional benefits

CONNECT WITH US

November 21, 2022 10:57 pm | Updated 10:57 pm IST

COMMENTS

SHARE

READ LATER

**The story so far:** The latest draft of the data protection law — the Digital Personal Data Protection Bill, 2022 (DPDP Bill, 2022) — has now been made open for public comments. This article deals with various themes within the Bill including data localisation requirements, whether children are considered as data principals, the regulatory framework of the Bill and the penalties it imposes.

The DPDP Bill, 2022 misses out on two main rights for data principals. The first is the right of data portability. The right to data portability allowed the data principal to receive in a structured format all the personal data they had provided to the data fiduciary and data that the data fiduciary generated on the data principal while processing for provisioning of its services. This empowered data principals by allowing them to choose between different platforms and enhanced competition between data fiduciaries to increase consumer welfare. For example, if the data principal was not satisfied with the social media platform they were currently using, they could request for porting of their data to another social media platform and avail of its services without having to provide all their personal data again. The DPDP Bill, 2022 does not provide for this right.

The second right foregone is the right to be forgotten. While not a right per se, the right to be forgotten allows the data principal to ask the data fiduciary to stop the continuing disclosure of their personal data. This has to be balanced with the right to freedom of speech and expression and the right to information for all other individuals. The DPDP Bill, 2022 subsumes this right under the right to erasure. This conflation between the general right to erasure with the right to be forgotten which is specific to disclosure of personal data compromises on the right to freedom of speech and expression of other individuals.

With regard to the personal data processing of children, the DPDP Bill, 2022 carries forward the approach of its previous iterations. A major issue that remains is that the age of digital consent, which is the age at which an individual can consent to their personal data being processed, continues to be 18. This means that parental/guardian consent would be required to process the personal data of children and adolescents below the age of 18 years. In effect, this would mean parental consent would be required every time they want to access the internet. This becomes an issue for three reasons. First, the high threshold of 18 years negates evolving capacity as it does not recognise that the consent of a toddler is different from that of a teenager. Second, it would result in unequal access to the internet and, finally, requiring consent from parents would

hamper autonomous development of children since parents may not want them to be exposed to viewpoints contradictory to their own. Such restrictions are in violation of India's obligations under the Convention on Rights of the Child.

One of the most emphatic departures of the DPDP Bill, 2022 from the Personal Data Protection (PDP) Bill 2019, has been in the context of cross border data flows. The PDP Bill, 2019 provided for a three-tiered categorisation based on which personal data could be moved across borders. While the government was interested in restricting cross border data flows of sensitive personal data and critical personal data to allow for ease of lawful access and to maintain "digital sovereignty", these data localisation requirements were severely contested by the industry as they would lead to significant increase in compliance and operational costs in terms of higher data storage charges and security risks.

The DPDP Bill, 2022 aims to strike a balance between these concerns by allowing for cross border data flow to "countries and territories" notified by the Central government. However, the draft legislation fails to provide any guidance or criteria for the consideration of the Union government while making this notification. The criteria is left to the Central government itself to be specified under its rule making power.

In comparison to the regulatory framework conceptualised under the previous iterations of the draft law, where the proposed regulator, the Data Protection Authority, was enshrined with significant powers of regulation making, enforcement and adjudication, the current draft considerably reduces the scope of the proposed Data Protection Board of India (DPB). Out of the 22 clauses in the DPDP Bill, the Central government has been provided with rule making power in around 14 clauses.

This becomes problematic for several reasons. First, the government forms one of the largest data fiduciaries in the country. It processes personal data of millions of Indians for provisioning of services and benefits, issuance of permits, licences and official IDs and for law enforcement generally. As such, it becomes important the agency making the rules should be at an arm's length from the government so as to ensure impartial protection of the interests of data principals. Vesting these powers with the Union government which would itself be subject to these rules creates conflict of interest. For example, the government has the power to specify "fair and reasonable" purposes for which it can process personal data without consent.

Similarly, it can make rules on data protection obligations of data breach, data protection impact assessments, data audits, information that can be requested from a data fiduciary which the government will itself be subject to in its capacity as a data fiduciary. Moreover, the DPDP Bill, 2022 fails to provide adequate legislative guidance for framing these rules. This leads to the concern of excessive delegation of legislation.

Lastly, the Central government exercises greater control over the proposed DPB because it will appoint members of the DPB, set out the terms and conditions of appointment and lay out the functions that the DPB will perform.

Carrying forward the approach from the PDP Bill, 2019, the current Bill also provides considerable exemptions to the state's processing of personal data. First, as stated above, the Union government has the power to specify "fair and reasonable" purposes for which it can process personal data without consent. Second, an exemption from most data protection obligations is provided if the processing is undertaken "in the interests of prevention, detection, investigation of *any* offence or any other contravention of any *law*" This may be in violation of the "necessity and proportionality" test laid down by the Supreme Court in *Puttaswamy vs Union of India*. A complete exemption can be provided for when personal data is being processed "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”. Lastly, and this is an addition to the PDP Bill, 2019, the Union government can now notify exemption to certain data fiduciaries based on just the “volume and nature of personal data” processed, irrespective of the purpose for which it is being processed.

Moreover, storage limitation does not apply to government agencies which means they can continue to retain personal data for an unlimited period of time even when the purpose of processing ceases to exist and there is no legal requirement to store the data.

The DPDP Bill, 2022 marks a number of departures from the PDP Bill, 2019 in the way it conceptualises penalties. First, the quantum of penalties that can be imposed, with the cap being placed at 500 crore, are of a much higher magnitude than provided for under the PDP Bill, 2019. Second, unlike the PDP Bill, 2019 the DPDP Bill, 2022 creates no offences. Third, in a move that can be seen as disempowering the data principals, the DPDP Bill, 2022 does not allow them to seek compensation from data fiduciaries for harms they have suffered due to unlawful processing. Fourth, in a very unusual move and perhaps the only one of its kind among data protection legislations, the DPDP Bill, 2022 places duties on data principals. If they are non-compliant, it could lead to penalties upto 10,000. Some of these duties include being in compliance with the “provision of *all* applicable laws” when exercising rights and not registering “false or frivolous” complaints with the data fiduciary or the DPB. Such provisions may hinder data principles from exercising their rights for fear of penalties.

*The writer is a research fellow at the Centre for Applied Law and Technology Research, Vidhi Centre for legal policy*

*(This is the second of a [two-part series](#) on the draft Digital Personal Data Protection Bill, 2022)*

COMMENTS

SHARE

[The Hindu Explains / Text and Context / computing and information technology / technology \(general\)](#)

BACK TO TOP

Comments have to be in English, and in full sentences. They cannot be abusive or personal. Please abide by our [community guidelines](#) for posting your comments.

We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

**END**

Downloaded from [crackIAS.com](#)

© **Zuccess App** by crackIAS.com