Bill on data protection gets Cabinet approval, to be presented in Parliament

Exemptions to govt entities from adverse consequences have likely been retained

The Union Cabinet Wednesday **approved the draft data protection Bill,** paving the way for its **introduction in the Monsoon session of Parliament.** If passed, the law will become India's core data governance framework, six years after the Supreme Court declared privacy as a fundamental right. The Bill is one of the four proposed legislations in the IT and telecom sectors to provide the framework for the rapidly growing digital ecosystem.

The **Digital Personal Data Protection Bill, 2022**, approved by the Cabinet, is learnt to have retained the contents of the original version of the legislation proposed last November, including those that were **red flagged by privacy experts.** Wide-ranging exemptions for the Central government and its agencies, remain unchanged. The Central government will have the right to exempt "any instrumentality of the state" from adverse consequences citing national security, relations with foreign governments, and maintenance of public order among other things.

The control of the Central government in appointing members of the Data Protection Board – an adjudicatory body that will deal with privacy-related grievances and disputes between two parties – is learnt to have been retained as well. The Chief Executive of the board will be appointed by the Central government, which will also determine the terms and conditions of their service.

The fresh draft was released following the withdrawal of an earlier version from Parliament last August after nearly four years in the works, where it went through multiple iterations, a review by a Joint Committee of Parliament (JCP), and pushback from a range of stakeholders including tech companies and privacy activists.

One of the key changes to the final draft of the Bill is learnt to be in the way it deals with cross-border data flows to international jurisdictions – by moving away from a whitelisting approach, to a blacklisting mechanism.

The Indian Express had earlier reported that in a move that could further liberalise conditions for data transfer, the proposed new law could allow global data flows by default to all jurisdictions other than a specified negative list of countries where such transfers would be restricted – essentially an official blacklist of countries where transfers would be prohibited.

The draft, which was released for public consultation in November, said the Central government will notify countries or territories where personal data of Indian citizens can be transferred, that is, a whitelist of jurisdictions where data transfers would be allowed.

A provision on "deemed consent" in the previous draft could be reworded to make it stricter for private entities while allowing government departments to assume consent while processing personal data on grounds of national security and public interest.

A senior government official said the Bill is expected to allow "voluntary undertaking" – meaning that entities that have violated provisions of law can bring it up with the Data Protection Board, which can decide to bar proceedings against the entity by accepting settlement fees. Repeat offences of the same nature could attract higher financial penalties, the official said.

The highest penalty that can be levied on an entity – in account of failing to prevent a data breach – has been prescribed to be Rs 250 crore per instance. In informal conversations, government officials have emphasised that the definition of "per instance" is subjective and could mean either an instance of a data breach, or account for the number of people impacted by it and multiply it by Rs

250 crore. None of this however, has been prescribed under law, and is open to interpretation by the data protection board on a case-by-case basis.

The implementation of the Bill will be “digital by design,” they said, insisting that “advanced” plans have been made by the government to that end. Consent requirements under the Bill could also force companies to change the way they serve up cookies on their websites, where they will have to seek specific consent on how the cookies might track a user’s activities on their site, the official said.