News: In a significant departure from the draft Bill, the **Personal Data Protection Bill** cleared by the Cabinet on Wednesday allows some personal data to be stored and processed abroad with the individual’s consent, without requiring a mirror of the data in India, official sources said.

Prelims and Mains focus: About the key changes made in the Bill and its significance, challenges in implementation

Background: After the public release of a draft Bill by a committee headed by Justice B N SriKrishna in July 2018, India was caught in the middle of a global debate on data localisation at the G20, the Organisation for Economic Co-operation and Development (OECD) and other fora.

Changes made in the draft of the Bill

A previous draft of the Bill required a copy of all personal data to be stored in India — a provision that was criticised by foreign technology companies and civil society stakeholders.

However, the Bill still requires “sensitive” personal data — related to financial, health, sexual orientation, biometric, genetic, transgender status, caste and religious belief — to be stored only in India.

This data can be processed abroad only under certain conditions, including the approval of a Data Protection Agency (DPA).

Moreover, “critical” personal data, as defined by the government from time to time, must be stored and processed only in India. These provisions will impact companies like Google, Facebook and WhatsApp, which currently store most of their India-related data abroad.

In another change, the **Bill mandates companies to give the government access to any non-**
personal data — anonymised data like traffic patterns or demographic information — which many companies use to fund their business model. The previous draft did not specify this.

The Bill also requires social media companies, which are deemed “significant data fiduciaries” (SDF) based on factors such as volume and sensitivity of data as well as their turnover, to develop their own user verification mechanism. While the process can be voluntary for users and can be completely designed by the company, it will decrease the anonymity of users and “prevent trolling.”

The Bill includes exemptions for processing data without an individual’s consent for “reasonable purposes”, including security of the state, detection of any unlawful activity or fraud, whistleblowing, medical emergencies, credit scoring, operation of search engines and processing of publicly available data.

While the Bill retains the provisions on a Data Protection Authority (DPA), the penalties listed are: Rs 5 crore or 2 per cent of worldwide turnover for minor violations and Rs 15 crore or 4 per cent of total worldwide turnover for more serious violations. Besides, the company’s executive-in-charge can also face jail term of up to three years.

Govt’s stand

The government will be entitled to give direction to the fiduciary to provide to the government anonymised, personal data and impersonal data for framing policy for better delivery of services and evidence-based policy.

Personal data processed in the interest of prevention, detection, investigation and prosecution of any offence is exempt. In the interest of sovereignty, national security, preventing communal violence, the govt. exempted some agencies from the law.

This Act will not deter the government from framing any policy for the growth of the digital economy, to the extent that it doesn’t impinge on personal data privacy.
Government sources said they were open to the “widest debate on this Bill”, which is expected to be tabled in Parliament during the ongoing Winter Session.