

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 3943
TO BE ANSWERED ON: 12.08.2026

IMPLEMENTATION OF RULES UNDER DPDP ACT, 2023

3943. SMT. JUNE MALIAH:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

- (a) whether the Government has finalized the implementation rules under the Digital Personal Data Protection Act, 2023;
- (b) if so, the timeline for rollout and enforcement; and
- (c) the details of safeguards being ensured to protect citizens' data from misuse and cyberattacks?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (c): The policies of the Government of India are aimed at ensuring an open, safe, trusted and accountable cyberspace for users in the country. Government of India has taken major initiatives like the enactment of the Information Technology Act, 2000 (IT Act), the setting up of the Indian Computer Emergency Response Team (CERT-In), the release of the National Cyber Security Policy 2013, and the enactment of the Digital Personal Data Protection Act 2023 (DPDP Act), thus ensuring security and protecting the privacy of users in India.

Information Technology Act, 2000 (IT Act):

- (i) The Information Technology (IT) Act, 2000 provides a technology-neutral legal framework governing electronic transactions, protection of computer resources, cybersecurity, intermediary due diligence and cyber offences.
- (ii) The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 prescribe due diligence obligations for intermediaries, including significant social media intermediaries, with a view to promoting a safe, trusted and accountable online environment.

Digital Personal Data Protection Act 2023 (DPDP Act):

- (i) DPDP Act 2023 provides for the processing of digital personal data in a manner that recognises both the rights of the individual to protect their personal data and the need to process such personal data for lawful purposes.
- (ii) The Act, and the Digital Personal Data Protection Rules, 2025 (“Rules”) notified on 13 November, 2025 provide a timeline for phased implementation of its provisions over an eighteen- month transition period, including the establishment of the Data Protection Board. The Rules specify the following implementation timelines:
 - Phase 1: Establishment and operationalisation of the Data Protection Board of India
 - Phase 2 (within one year): Registration and functioning of Consent Managers

- Phase 3 (within eighteen months): Compliance obligations for Data Fiduciaries including data principal rights, security safeguards and breach notification
- (iii) The Act requires all Data Fiduciaries to ensure lawful processing of personal data. It lays down clear obligations relating to transparency, purpose limitation, data minimization, accuracy, security safeguards and respect for the rights of Data Principals.
- (iv) It requires Data Fiduciaries to implement strong security safeguards, erase personal data upon withdrawal of consent (unless retention is legally required), and comply within the transition period.
- (v) The Rules further require Data Fiduciaries to adopt appropriate technical and organizational safeguards, such as encryption or masking, to protect personal data and prevent breaches. The Act envisages the Data Protection Board to address violations of the Act. It can investigate breaches, issue corrective directions, and impose penalties. Penalties are to be determined based on factors like the nature of the breach, harm caused, safeguards in place, severity, and recurrence.
- (vi) In the event of a personal data breach, Data Fiduciaries are required to promptly notify the affected Data Principals and the Data Protection Board of India. Upon receipt of breach intimation, the Data Protection Board may conduct an inquiry and impose monetary penalties in accordance with the Act.
- (viii) The Board is empowered to investigate breaches, issue corrective directions, and impose penalties up to ₹250 crore, taking into account factors like nature of breach, harm caused, safeguards in place, severity and recurrence.

Public Awareness Activities:

- (i) The Government is implementing the Information Security Education and Awareness (ISEA) project to build human resources in information security and promote awareness on cyber hygiene and cyber security among citizens.
- (ii) Under the ISEA project, over 6,650 awareness workshops have been conducted across the country, covering more than 11.37 lakh participants, including school and college students, teachers, law enforcement personnel, government officials and the general public.
- (iii) Multilingual awareness material, including handbooks, short videos, posters, brochures and cartoon stories for children, has been developed and disseminated through print, electronic and social media, as well as through the ISEA and Stay Safe Online portals i.e. www.isea.gov.in & <https://staysafeonline.in/>.
- (iv) The Government also organises nationwide awareness campaigns such as Cyber Security Awareness Month and Safer Internet Day to promote safe online behaviour, secure digital transactions and responsible use of digital services.
- (v) Cyber security advisories are issued regularly on emerging cyber threats, mitigation strategies and best practices. Initiatives such as the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) and the National Cyber Coordination Centre (NCCC) strengthen cyber resilience by detecting and mitigating malicious activities and enhancing situational awareness.
- (vi) Indian Computer Emergency Response Team (CERT-In) regularly disseminates cyber safety and security advisories, awareness posters, infographics and videos through its official website and social media platforms to sensitise internet users about cyber threats, online frauds and safe online practices, including online safety measures for children.
- (vii) The Ministry of Education issued the PRAGYATA Guidelines on Digital Education in July 2020, providing a framework for safe and effective online learning, including the promotion of students' well-being and responsible use of social media and digital devices.

(viii) The Central Board of Secondary Education (CBSE) has supplemented these efforts by issuing guidelines on digital etiquette, conducting cyber security training for teachers, publishing the Cyber Security Handbook, and advising schools to establish Cyber Clubs to promote cyber safety awareness.

(ix) The National Council of Educational Research and Training (NCERT) has integrated cyber safety into the school curriculum, including a chapter on "Societal Impacts" for Classes XI and XII. In addition, CIET-NCERT has developed and disseminated educational resource materials on cyber safety.

(x) The Government has taken various measures to promote widespread awareness and adoption of the Digital Personal Data Protection (DPDP) Act by educating citizens on their rights & duties and capacity-building initiatives, including workshops, conferences, expert sessions, and digital outreach campaigns.
