

GOVERNMENT OF INDIA  
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY  
**LOK SABHA**  
**UNSTARRED QUESTION NO. 5123**  
TO BE ANSWERED ON: 02.04.2025

**IMPLEMENTATION OF DPDP ACT, 2023**

**5123. MS. S JOTHIMANI:**

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

- (a) the status of the implementation of the Digital Personal Data Protection Act, 2023;
- (b) the manner in which the Government is addressing concerns about data privacy and security in digital platforms;
- (c) the measures in place to combat cybercrime, online fraud and ransomware attacks;
- (d) the manner in which the Ministry is ensuring the security of Government data and critical infrastructure; and
- (e) the steps being taken by the Government to prevent data leaks and safeguard citizens' personal information?

**ANSWER**

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

(a) to (e): The Digital Personal Data Protection Act, 2023 (DPDP Act) has been enacted on 11<sup>th</sup> Aug 2023. The Ministry has notified draft Digital Personal Data Protection Rules, 2025 (Rules) for public consultation, which seek to operationalize the DPDP Act. Feedback comments from public including stakeholders have been invited in line with the Government's commitment of inclusive approach towards law-making.

The DPDP Act 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.

The Government of India has undertaken a multi-faceted approach to ensure protection of digital personal data. The Government has also taken several measures for improving cyber security & data privacy of data platforms including critical infrastructure. These include:

- i. National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) ensures coordination amongst different agencies.
- ii. Under the provisions of section 70B of the Information Technology (IT) Act, 2000, the Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents.

- iii. National Cyber Coordination Centre (NCCC) implemented by the CERT-In detects cyber security threats. NCCC facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate cyber security threats.
- iv. Cyber Swachhta Kendra (CSK) is a citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space. Cyber Swachhta Kendra is the Botnet Cleaning and Malware Analysis Centre and helps to detect malicious programs and provides free tools to remove the same. It also provides cyber security tips and best practices for citizens and organisations.
- v. Ministry of Home Affairs (MHA) has created the Indian Cybercrime Coordination Centre (I4C) to deal with cybercrimes in a coordinated and effective manner.
- vi. Under the provisions of section 70A of the IT Act, 2000, the Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country.
- vii. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under the IT Act prescribes reasonable security practices and procedures to protect sensitive personal data of users.
- viii. Capacity building and awareness are integral components of the Government's IT security strategy. Training programs are conducted across sectors, focusing on developing IT security skills among officials and professionals. Public awareness campaigns, such as Cyber Security Awareness Month and Safer Internet Day, are organized to educate citizens about online safety, secure online transactions and digital services.
- ix. The cyber security advisories are regularly issued on emerging threats, mitigation strategies, and best practices to safeguard data. Initiatives like the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) and the National Cyber Coordination Centre (NCCC) focus on detecting and mitigating malicious activities, enabling situational awareness, and securing against potential threats.
- x. A significant step in this direction is the enactment of the DPDP Act, which establishes the legal framework for data protection and mandates data fiduciaries to implement comprehensive security safeguards in India. DPDP Act establishes the grievance redressal mechanism and adjudication process of the Data Protection Board, digital by design in nature, with a robust framework of accountability mechanisms to ensure the lawful processing of digital personal data with Data Protection Board as an independent adjudicatory body empowered to investigate complaints, conduct inquiries, and impose penalties for non-compliance of the provisions of the Act.

\*\*\*\*\*

