GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 710
TO BE ANSWERED ON: 25.07.2025

IMPLEMENTATION OF DPDP RULES, 2025

710. SHRI RAVI CHANDRA VADDIRAJU:

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

(a) whether the draft Digital Personal Data Protection (DPDP) Rules, 2025, are being implemented across the country, if so, the details thereof, if not, the reasons therefor;
(b) the number of public feedback/submissions received on these rules;
(c) whether awareness programs are conducted to educate citizens, if so, the details thereof, if not, the reasons therefor; and
(d) whether steps are being taken to ensure data security, if so, the details thereof, if not, the reasons therefor?

ANSWER

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

(a) to (d): The Digital Personal Data Protection (DPDP) Act, 2023 is a comprehensive data privacy law to regulate the processing of digital personal data. It balances the rights of individuals to protect their personal data with the need for lawful data processing.

Draft Digital Personal Data Protection Rules, 2025, which aim to operationalize the act, were published for public consultation. 6,915 feedback/inputs have been received from citizens and stakeholders.

The policies of Government of India are aimed at ensuring a safe, trusted, and accountable cyberspace for all users. Capacity building and awareness are important components of the Government's IT security strategy:

- Regular training programs are conducted across sectors to build IT security skills among officials and professionals
- Public awareness campaigns such as *Cyber Security Awareness Month* & *Safer Internet Day* promote online safety, secure digital transactions, & cyber hygiene
- CyberShakti programme, launched in October 2024, aims to build a skilled women workforce in cybersecurity
- Under Information Security Education and Awareness (ISEA) programme, 3,637 workshops have been conducted, reaching over 8.2 lakh+ participants, including academia, law enforcement, government personnel, women, and the general public

- Multilingual awareness materials such as handbooks, videos, posters, and advisories (including on deepfakes) are widely disseminated.
- Awareness resources are available on platforms like www.staysafeonline.in, www.infosecawareness.in, and www.csk.gov.in.

Some of the key measures taken by government to strengthen cybersecurity are as follows:

- Establishment of National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country (Section 70A of IT Act, 2000)
- Indian Computer Emergency Response Team (CERT-In) designated as the national agency for responding to cyber security incidents (Section 70B of IT Act)
- Cyber security advisories are regularly issued by CERT-In on emerging threats, mitigation strategies, and best practices to safeguard data
- National Cyber Coordination Centre (NCCC) implemented by the CERT-In detects cybersecurity threats, facilitates coordination among different agencies by sharing with them the information to mitigate cybersecurity threats.
- National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) ensures coordination amongst different agencies.
- Cyber Swachhta Kendra (CSK), a citizen-centric service & Botnet Cleaning and Malware Analysis Centre, provided by CERT-In, helps to detect malicious programs and provides free tools to remove them.
    - It also provides cyber security tips and best practices for citizens and organisations.
- 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.
- Digital Personal Data Protection (DPDP) Act, provides a comprehensive framework for the protection of digital personal data of individuals while making Data Fiduciaries accountable for personal data breaches.

    - Data fiduciaries are required to implement appropriate technical & organizational measures to prevent personal data breaches by taking reasonable security safeguards.

****