GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1352
TO BE ANSWERED ON: 06.12.2024

STATUS OF IMPLEMENTATION OF DPDP ACT

1352. SMT. RANJEET RANJAN:
SHRI HARIS BEERAN:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY:

(a) the status of the implementation of the Digital Personal Data Protection (DPDP) Act, 2023, including the establishment of the Data Protection Board and the issuance of the DPDP Rules;
(b) whether Government has considered restricting the exemptions provided to State agencies under the Digital Personal Data Protection (DPDP) Rules with respect to the fundamental right to privacy;
(c) if so, the details thereof, if not, the reasons therefor; and
(d) the steps being taken by Government to enhance cybersecurity infrastructure in light of the projected increase in cyberattacks and data leaks?

ANSWER

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

(a) to (c): The Digital Personal Data Protection Act, 2023 (DPDP Act) received the assent of the Hon'ble President on 11th August 2023. Elaborate discussions and consultations have been done with various stakeholders including industry bodies, civil societies, government organizations etc. while drafting the Rules. The drafting of the Rules is in the final stage. The establishment of the Data Protection Board is a subsequent step after the notification of the Rules. The Rules are being drafted in line with the provisions of the Act.

(d): The Government of India has undertaken a multi-faceted approach to enhance cybersecurity infrastructure in response to the growing threats of cyberattacks and data breaches. Some of the major initiatives includes enactment of Information Technology Act, 2000 (“IT Act”) and setting up of Indian Computer Emergency Response Team (CERT-In) and National Critical Information Infrastructure Protection Centre (NCIIPC) under the IT Act, release of National Cyber Security Policy 2013, appointment of Chief Information Security Officer (CISO), Cyber Crisis Management Plan (CCMP) for countering cyber attacks and cyber terrorism, promotion of cyber security industry in the country, promotion of cyber security R&D and capacity building in Cyber Security.

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 take reasonable security safeguards to prevent personal data breaches. The DPDP Act requires Data Fiduciaries to process personal data for lawful purposes only, prevent personal data breaches, notify personal data breach to Data Protection Board and affected individuals and implement appropriate technical and organizational measures.

The Indian Computer Emergency Response Team (CERT-In), established under Section 70B of the Information Technology Act, 2000, serves as the national nodal agency for cybersecurity. CERT-In has mandated reporting of cybersecurity incidents, including breaches, phishing, and ransomware attacks, by entities such as service providers, intermediaries, and government organizations. It regularly issues advisories 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 networks against potential threats.

Capacity building and awareness are integral components of the Government's cybersecurity strategy. Training programs are conducted across sectors, focusing on developing cybersecurity 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 digital payments, and protection against phishing and fraud.

Policy measures, including the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, ensure that sufficient measures are adopted by intermediaries to safeguard user data and promptly address grievances. Non-compliance results in the loss of safe harbor protections under Section 79 of the IT Act, ensuring accountability for intermediaries.
By integrating legal, technical, and collaborative measures, the policies of Government of India are aimed at ensuring an open, safe, trusted and accountable cyberspace for users in the country.

****