GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
**LOK SABHA**
**UNSTARRED QUESTION NO. 1649**
TO BE ANSWERED ON: 30.07.2025

## MEASURES TO PROTECT CITIZENS' DATA

**1649. SHRI VISHALDADA PRAKASHBAPU PATIL:**

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

(a) the status of the Personal Data Protection Bill as of July 2025 and its expected enactment timeline;
(b) the manner in which the Government balances data privacy with digital economy growth given 1.4 billion digital transactions monthly;
(c) the details of measures to protect citizens' data with over 1,200 cyber incidents reported in 2024;
(d) the details of the economic impact assessment of data localization requirements on businesses; and
(e) the details of international agreements on data protection and cybersecurity in 2025?

## 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 11th August, 2023. It establishes a framework for processing digital personal data, balancing the rights of individuals to protect their data with the need for lawful data processing. Draft Digital Personal Data Protection Rules, 2025 (Rules) which seek to operationalize the Act have been published for public consultation. DPDP Act and draft Rules are available on the ministry website. Until the DPDP Act comes into force, the provisions of Section 43A of the IT Act, read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 continue to apply for the protection of sensitive personal data or information.

The Government has undertaken several initiatives to enhance cyber security standards, strengthen digital infrastructure, and promote cybersecurity awareness, with the objective of ensuring an Open, Safe, Trusted, and Accountable Internet for all users. Government remains cognizant and aware of cyber threats and challenges. Following measures have been taken to strengthen cybersecurity in the country:

i. With participation from the government, industry, and academia, the Bureau of Indian Standards (BIS) formulates cybersecurity standards through its technical committees. These committees also serve as the National Mirror Committees for the corresponding international committees of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). India's active role in international standardization efforts fosters collaboration with global partners, provides early insights into emerging developments, promotes alignment with evolving best practices, and strengthens national cybersecurity capabilities.

ii. The Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents under the provisions of section 70B of the Information Technology Act, 2000.

iii. The Government has established the National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country under the provisions of section 70A of the Information Technology (IT) Act, 2000.

iv. CERT-In works with other agencies involved in ensuring cybersecurity including Telecom Security Operations Centre (TSOC), India Cyber Crime Coordination Centre (I4C), National Centre Information Infrastructure Protection Centre (NCIIPC), etc.

v. CERT-In along with other agencies was able to successfully prevent cyber-attacks during the G20 summit, Parliament 20 summit, Ram Janmabhoomi event, Maha Kumbh etc.

vi. Regular training workshops are conducted for cybersecurity professionals, Chief Information Security Officers(CISO) and government employees etc.

vii. CERT-In operates an automated cyber threat intelligence exchange platform for sharing tailored alerts with organisations across sectors for proactive threat mitigation.

viii. Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors.

ix. 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, and also provides cyber security tips and best practices for citizens and organisations.

x. CERT-In has formulated Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism for implementation by all Ministries/ Central Government Departments, State Governments and their organizations and critical sectors.

xi. CERT-In has empaneled 200 security auditing organizations to support and audit implementation of Information Security Best Practices.

xii. Computer Security Incident Response Team in Finance sector (CSIRT-Fin) under CERT-In is operational since May 2020 to coordinate cyber incident response in the banking and financial sector.

xiii. MeitY observes the Cyber Security Awareness Month (NCSAM) during October of every year, Safer Internet Day on 2nd Tuesday of February every year, Swachhta Pakhwada from 1st to 15th February of every year and Cyber JagrooktaDiwas (CJD) on 1st Wednesday of every month by organising various events and activities for citizens as well as the technical cyber community in India

Certain sectoral regulators such as Reserve Bank of India and Securities Exchange Board of India have introduced norms for storing certain data within India. Impact assessments of such norms, if any, have not been shared with the Ministry of Electronics and IT.

Government of India has not signed any international agreement on data protection and cybersecurity in 2025.

******