GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION. NO. 3217
TO BE ANSWERED ON: 19.03.2025

INCIDENTS OF DATA BREACH IN THE IT SECTOR

3217. SHRI BIDYUT BARAN MAHATO:
SHRI ARUN GOVIL:

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

(a) the steps taken by the Government to implement robust data protection regulations to ensure security and privacy of personal information of citizens in India in view of the increasing incidents of data breach in the IT sector and concerns over data privacy; and
(b) the initiatives being taken by the Government to raise awareness among people about their digital rights and hold technology companies accountable for any violation of data privacy and security rules, especially in view of increasing online transactions and digital services?

ANSWER

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

(a) and (b): The Government of India has undertaken a proactive approach to strike a unique balance between fostering innovation and regulation to protect digital personal data in response to increasing digitization. Government of India has taken major initiatives like enactment of Information Technology (IT) Act, 2000, setting up of Indian Computer Emergency Response Team (CERT-In) and National Critical Information Infrastructure Protection Centre (NCIIPC), releasing of National Cyber Security Policy 2013, appointing Chief Information Security Officer (CISO) ensuring security and privacy of personal information of citizens in India.

Additionally, a significant step in this direction is the enactment of the Digital Personal Data Protection Act, 2023 (‘DPDP Act’), which establishes the legal framework for data protection and mandates data fiduciaries to implement comprehensive security safeguards in India. The Act requires fiduciaries to process personal data responsibly, notify breaches promptly, and ensure accountability through technical and organizational measures.

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. The cyber security advisories are regularly issued on emerging threats, mitigation strategies, and best practices to safeguard data. Intiatives 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.

******