GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION. NO. 3903
TO BE ANSWERED ON: 18.12.2024

LEAKAGE OF PERSONAL DATA

†3903. SHRI SUKHJINDER SINGH RANDHAWA:

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

(a) whether it is a fact that the Government has completely failed to prevent the leakage of personal data due to which cyber crimes are increasing day by day;
(b) if so, the steps taken/proposed to be taken by the Government to keep personal data information secure; and
(c) whether the Government has identified information/leakage sources of personal data, if so, the details of the action taken against them and if not, the reasons therefor?

ANSWER

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

(a) to (c): The Government is committed to ensure that internet in India is open, safe, trusted and accountable for its users. Government is fully cognizant and aware of various cyber threats and challenges. To strengthen the nation's cybersecurity posture and enable the protection of personal data, the Government has taken several key initiatives which, inter alia, includes:

i. 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.
ii. CERT-In issued Cyber Security Directions in April 2022 under sub-section (6) of section 70B of Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet. On observing cyber security incidents, CERT-In advises remedial measures to concerned organisations.
iii. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data on an ongoing basis.
iv. CERT-In has issued an advisory to various Ministries outlining the measures to be taken for strengthening the cyber security by all entities that are processing the digital personal data or information including sensitive personal data or information.
v. 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.
vi. CERT-In has formulated a Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.
vii. Unique Identification Authority of India (UIDAI) has put comprehensive measures in place to protect the personal data of Aadhaar number holders. It has implemented multi-layered security infrastructure with defence-in-depth concept to protect the Central Identities Data

Repository (CIDR) database and continuously reviews/audits the same to protect UIDAI systems. Further, CIDR is declared as a protected system and the National Critical Information Infrastructure Protection Centre provides security inputs on an ongoing basis to maintain its cybersecurity posture. UIDAI uses advanced encryption technologies for protecting data in transmission and storage.

viii. National Cyber Coordination Centre (NCCC) implemented by the CERT-In serves as the control room to scan the cyberspace in the country and detect 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.

ix. National Informatics Centre (NIC) mandates periodic security audits of government websites, applications and hosting infrastructure through CERT-In-empanelled agencies to eliminate vulnerabilities and ensure compliance with global security standards.

x. CERT-In issued Guidelines for Secure Application Design, Development, and Implementation & Operations in September 2023. CERT-In has also released the Software Bill of Materials (SBOM) guidelines for entities, particularly those in the public sector, government, essential services, organizations involved in software export and software services industry in October 2024 to help organizations know exactly what components are in their software or assets, making it easier to identify and fix vulnerabilities.

xi. CERT-In has empanelled 155 security auditing organisations to support and audit implementation of Information Security Best Practices.

xii. To ensure that the technology deployed by the authorized Payment System Operators (PSOs) to operate the payment system/sin a safe secure, sound, and efficient manner, Reserve Bank of India (RBI) had directed all PSOs to get Audit of their payment system done by CERT-In empanelled auditors on an annual basis and submit the report to RBI within two months of close of their respective financial year.

xiii. In order to ensure data protection, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011 ('SPDI Rules') mandates reasonable security practices and procedures for compliant body corporate or any person on its behalf, handling sensitive personal data or information. Body corporate or any person on its behalf shall obtain written consent from the provider of such information regarding lawful purpose of usage before collection of such information.

xiv. Further, in order to safeguard the personal data of individuals and ensure that their data is shared only with their consent, the Digital Personal Data Protection Act, 2023 (DPDP Act) has been enacted. The DPDP Act is aimed at safeguarding the personal data of individuals, including consumers in the e-commerce sector and ensuring processing of personal data for the lawful purposes. The DPDP Act mentions that appropriate technical and organisational measures must be implemented for processing of the personal data and reasonable security safeguards must be taken to prevent any personal data breach.

****