GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
**LOK SABHA**
**UNSTARRED QUESTION NO. 5285**
TO BE ANSWERED ON: 02.04.2025

# LEAKAGE OF AADHAAR DATA

**5285. SHRI ESWARASAMY K:**

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

(a) the steps taken by the Government for the protection against leakage of data submitted to Government authorities like Aadhaar data under UIDAI;
(b) the action taken against employees found to be guilty of leaking data of individuals or citizens to unauthorized persons; and
(c) whether it is a fact that the Government has set up a committee for data protection and drafting of Data Protection Bill and if so, the details thereof?

## ANSWER

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

(a) to (c): Aadhaar is the world's largest biometric identity system comprising more than 133 crore individuals and has completed more than 13,000 crore authentication transactions.

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Act") mandates every authentication user agency to ensure that the identity information of the Aadhaar number holders collected during authentication and any other information generated during the authentication process is kept confidential, secure and protected. The Act and guidelines issued by Unique Identification Authority of India provide for measures for protection of data and privacy of residents, while enabling residents better access to public and financial services.

The Information Technology Act, 2000 read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 prescribes reasonable security practices and procedures to protect sensitive personal data of users.

Digital Personal Data Protection Act, 2023 ("DPDP Act"), enacted on 11th August, 2023 after an extensive public consultation and deliberations, provides the legal framework for processing of personal data with reasonable safeguards for its protection. Further, the DPDP Act establishes a robust framework of accountability mechanisms to ensure lawful processing of digital personal data and in the event of personal data breaches empowering Data Protection Board of India to investigate complaints, conduct inquiries, and impose penalties as an independent adjudicatory body.

In addition, Government has taken following measures to enhance cyber security posture and prevent data leaks:

i. National Cyber Security Coordinator (NCSC) under the National Security Council Secretariat (NSCS) ensures coordination amongst different agencies.

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

iii. National Cyber Coordination Centre (NCCC) implemented by the CERT-In detects 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.

iv. Ministries/Organisations are sensitized regarding 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. Guidelines have been issued by CERT-In on information security practices for government entities covering domains such as data security, network security, identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and security auditing and also for Secure Application Design, Development, and Implementation & Operations.

vi. An automated cyber threat intelligence exchange platform is being operated by CERT-In for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

vii. 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. It also provides cyber security tips and best practices for citizens and organisations.

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. Regular training programmes are conducted for network and system administrators and Chief Information Security Officers of government and critical sector organisations regarding securing information technology infrastructure and mitigating cyber-attacks.

******