GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 4234
TO BE ANSWERED ON: 18.03.2026

DATA BREACH INCIDENTS

† 4234. SHRI RAJESH RANJAN:

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

(a) the number of data breach incidents reported to CERT-In during the last three years;
(b) the number of incidents related to Government databases or entities handling Aadhaar-related data along with the details of actions taken thereon;
(c) the number of times cyber security audits of Government databases and digital public infrastructure were conducted during the last three years;
(d) the number of penalties or enforcement actions imposed for failure to report or prevent data breaches; and
(e) the details of mechanisms established for co-ordination between Ministries and agencies to deal with large-scale data breach incidents?

ANSWER

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

(a) to (e): The policies of Government of India aim to ensure an open, safe, trusted, and accountable Internet for all users.

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.

No breach of data has occurred from the Central Identities Data Repository (CIDR) maintained by the Unique Identification Authority of India (UIDAI).

CERT-In has empanelled 237 security auditing organisations to support and audit implementation of Information Security Best Practices. A total number of cyber security audits conducted by CERT-In empanelled auditing organizations for Government entities, including State Government and Public Sector entities during last three years are as follows:

Year	**Total Audits**

2023	9772
2024	12176
2025	18667

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.

As per the Digital Personal Data Protection Act, 2023 (DPDP Act), 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.

Further, in the event of any such breach or complaint by the Data Principal with respect to exercise of her rights, the Data Protection Board after an inquiry, may impose monetary penalty as per the provisions of the Act.
The Act prescribes different monetary penalties for different types of breaches of the Act, with the maximum penalty upto two hundred and fifty crore rupees.

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

******