

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1622
TO BE ANSWERED ON: 29.07.2026

MEASURES TO REINFORCE TRUST IN DIGITAL GOVERNANCE SYSTEM

1622. THIRU DR. S JAGATHRATCHAKAN:

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

- (a) the details of issues arising from digital governance initiatives involving integration of identity systems in consumer devices including implications for privacy, user consent, data security, individual autonomy and protection of personal information;
- (b) the details of safeguards established by the Government for ensuring secure collection, storage and processing of data, preventing misuse of personal information and protecting user privacy within digital governance ecosystems;
- (c) the details of progress achieved through efforts directed towards strengthening transparency, accountability and responsible use of digital identity-related technologies across public-facing digital platforms and services;
- (d) the details of regulatory and institutional mechanisms adopted by the Government for monitoring compliance with data protection requirements and addressing concerns relating to privacy and user rights; and
- (e) the details of measures proposed by the Government for reinforcing trust in digital governance systems, improving transparency standards and ensuring citizen-centric implementation of technology-driven public services?

ANSWER

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

(a) to (e): The Government recognizes that digital governance initiatives involving the integration of identity systems in consumer devices must be implemented in a manner that safeguards privacy, security and the rights of individuals. The issues arising from the integration of identity systems in consumer devices primarily relate to informed consent, purpose specific use of data, secure transmission and storage, prevention of unauthorised access or disclosure, protection of biometric and personal information and preservation of individual choice. Accordingly, the Government has enacted the Information Technology Act (IT Act) , Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and the Digital Personal Data Protection Act, 2023 (DPDP Act), to establish a robust legal framework that promotes trust, transparency, accountability and the responsible use of digital identity-related technologies across public-facing digital platforms and services while safeguarding privacy and protecting personal data.

Information Technology Act, 2000 (IT Act):

(i) The Information Technology (IT) Act, 2000 provides a technology-neutral legal framework governing electronic transactions, protection of computer resources, cybersecurity, intermediary due diligence and cyber offences.

(ii) Under Section 43A of the IT Act, the Government has notified the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules), prescribing reasonable security practices and procedures for the protection of sensitive personal data or information.

(iii) The SPDI Rules require body corporates handling sensitive personal data or information to implement reasonable security practices and procedures commensurate with the nature of their business and the value of the information assets, and to demonstrate compliance in the event of an information security breach.

(iv) Under Section 70B of the IT Act, the Indian Computer Emergency Response Team (CERT-In) has been designated as the national agency for responding to cybersecurity incidents. CERT-In also operates the National Cyber Coordination Centre (NCCC) for detection, analysis and coordinated response to cybersecurity threats.

(v) Under Section 70A of the IT Act, the Government has established the National Critical Information Infrastructure Protection Centre (NCIIPC) to protect the nation's critical information infrastructure from cyber threats.

(vi) Moreover, the Government has prescribed stringent security requirements for the empaneled cloud service providers who are handling government data including compliance with international security and privacy standards along with other security requirements to ensure cloud security, service management, and data protection. These compliances and standards cover critical security aspects such as risk assessment, security controls, service delivery, incident management, intrusion detection, data privacy, log retention, data encryption, access control, etc.

Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016:

(i) The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and the regulations framed thereunder provide safeguards for Aadhaar authentication, including protection of core biometric information and security of identity data. Aadhaar authentication is voluntary except where its use is mandated under law.

(ii) The Aadhaar ecosystem incorporates multiple safeguards, including informed consent, purpose limitation, secure transmission of authentication requests, encryption of data, and strict controls on the collection, storage and sharing of personal information. The Aadhaar Act prohibits the sharing of core biometric information and restricts the use and disclosure of identity information except as provided under the Act.

(iii) UIDAI does not collect or store the purpose of authentication or the details of the transaction for which authentication is sought. Authentication responses are limited to a "Yes/No" response or e-KYC, as applicable, and are provided only with the resident's consent.

Digital Personal Data Protection Act, 2023 (DPDP Act):

The Government is implementing the DPDP Act and the DPDP Rules, 2025 in a phased manner. The measures include enforcement of security obligations on Data Fiduciaries, effective grievance redressal, mandatory reporting of personal-data breaches, remedial action and penalties through the Data Protection Board of India and continued compliance with prescribed security and privacy standards. These measures are intended to strengthen citizen trust, improve transparency and ensure secure delivery of digital public services.

(i) DPDP Act, 2023 provides a comprehensive legal framework for processing digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such data for lawful purposes.

(ii) To operationalise the Act, the Digital Personal Data Protection Rules, 2025 were notified on 13 November 2025.

(iii) The Act permits the processing of personal data for lawful purposes either on the basis of the consent of the Data Principal or for certain legitimate uses specified under the Act.

(iv) Where processing is based on consent, such consent must be free, specific, informed, unconditional and unambiguous, and must be preceded or accompanied by a notice specifying the personal data to be processed and the purpose of such processing.

(v) The Act places obligations on Data Fiduciaries (entities that determine the purpose and means of processing personal data) to:

- implement reasonable security safeguards to protect personal data;
- establish effective grievance redressal mechanisms; and
- notify the Data Protection Board of India and affected Data Principals in the event of a personal data breach.

(vi) The Act establishes the Data Protection Board of India to inquire into personal data breaches and other contraventions of the Act, direct remedial measures, and impose monetary penalties. It also provides for grievance redressal mechanisms and enforcement of the rights of Data Principals, thereby strengthening privacy protection and safeguarding user rights.

These measures are aimed at enhancing trust, protecting user rights and ensuring secure delivery of digital services.
