

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 3255
TO BE ANSWERED ON: 20.03.2026

SAFEGUARDS FOR DATA COLLECTION AND AUDIT OF COMPLIANCE

3255. SMT. JEBI MATHER HISHAM:

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

- (a) whether Government has comprehensively assessed risks of cyber data theft, misuse or privacy breaches from widespread Artificial Intelligence (AI) enabled CCTV deployment, taking into account the Supreme Court judgment on data privacy/right to privacy;
- (b) the details of safeguards governing data collection, storage, retention and destruction and the manner in which compliance is audited across public and private operators;
- (c) whether AI-based surveillance systems are subject to independent oversight, algorithmic bias audits and periodic legality review; and
- (d) whether grievance redressal, penalty and compensation mechanisms exist for individuals affected by the misuse of surveillance data?

ANSWER

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

(a) to (d): The policies of the Government of India aim to ensure an open, safe, trusted, and accountable cyberspace for users.

The Government recognises the rapid expansion of digital platforms and digital services across the country. This expansion has led to increased collection and processing of personal data. It has also raised concerns related to privacy, cyber data theft, and misuse of personal information.

There are additional concerns arising from the widespread deployment of AI-enabled CCTV systems. To address these issues, the Government enacted the Digital Personal Data Protection Act, 2023.

The Act provides a comprehensive legal framework for the processing of digital personal data. The Act is based on constitutional principles laid down by the Hon'ble Supreme Court.

In Justice K. S. Puttaswamy (Retd.) v. Union of India, the right to privacy was recognised as a Fundamental Right. The judgment emphasised the need for a statutory data protection framework.

To operationalise the Act, the Digital Personal Data Protection Rules, 2025 were notified on 13 November 2025. They provide procedural and implementation guidance under the Act.

The Rules also establish compliance requirements and institutional mechanisms. These include the Data Protection Board of India.

The key features of the framework are as follows:

- **Comprehensive legal framework:** The Act establishes a comprehensive framework governing the processing of digital personal data by both Government and private entities
This balances the right of individuals to protect their personal data with the legitimate need to process such data for lawful purposes
- **Core data protection principles:** The framework incorporates key principles including lawful processing, purpose limitation, data minimisation, accuracy of data, storage limitation, reasonable security safeguards and accountability
- **Consent and lawful processing:** Personal data may be processed only for lawful purposes, either on the basis of the consent of the individual (Data Principal) or for certain legitimate uses specified under the Act
Consent must be obtained through a clear and plain notice specifying the personal data to be processed, the purpose of processing and the manner in which the Data Principal may exercise her rights
- **Obligations of Data Fiduciaries:** Entities determining the purpose and means of processing personal data (Data Fiduciaries) are required to ensure lawful, fair and transparent processing
They must collect only such personal data as is necessary for the specified purpose and implement appropriate technical and organisational measures, including reasonable security safeguards, to prevent personal data breaches
- **Data retention and erasure:** The Act incorporates the principle of storage limitation, requiring Data Fiduciaries to retain personal data only for as long as necessary to fulfil the purpose for which it was collected or as required under law
Once the purpose has been fulfilled, such data must be erased unless its retention is mandated by law
- **Rights of Data Principals:** The Act provides individuals with specific rights, including the right to obtain information regarding personal data being processed, the right to correction and erasure of personal data and the right to grievance redressal
- **Security safeguards:** The Rules prescribe minimum security safeguards for the protection of digital personal data, including measures such as encryption, masking or tokenisation of personal data, controlled access to computing resources, logging and monitoring of access, backup and recovery mechanisms and contractual safeguards requiring Data Processors to adopt equivalent security controls
- **Personal data breach notification:** In the event of a personal data breach, Data Fiduciaries are required to notify the affected Data Principals as well as the Data Protection Board of India, along with details of the nature of the breach, its potential consequences and the remedial measures being undertaken
- **Regulatory oversight and penalties:** The Data Protection Board of India is empowered to adjudicate complaints, investigate breaches, determine instances of non-compliance and impose monetary penalties for contraventions of the Act, which in certain cases may extend up to ₹250 crore
- **Compensation mechanism:** Under the Digital Personal Data Protection Act, 2023, instances of non-compliance with obligations relating to personal data may be adjudicated by the Data Protection Board, which is empowered to take appropriate action in accordance with the Act

In cases where an individual suffers harm or civil injury due to misuse of personal data or violation of legal obligations, the individual may seek appropriate remedies, including compensation, before competent courts or other forums under applicable laws

Further, the India AI Governance Guidelines provide a complementary national framework to ensure that artificial intelligence systems are safe, trustworthy, human-centric and inclusive, while promoting innovation and economic growth.

These guidelines emphasise principles such as trust, fairness, accountability, transparency and safety in the development and deployment of AI systems.

Taken together, the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025 and the AI governance framework establish a robust regulatory architecture for the responsible processing of digital personal data.

These are aimed at safeguarding the privacy and rights of individuals while fostering a secure and innovation-driven digital ecosystem in the country.
