GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 3902
TO BE ANSWERED ON: 04.04.2025

INITIATIVES FORESTABLISHMENT OFDATACENTRES

3902. **SHRIPARIMALNATHWANI:**

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:
(a) Government'sinitiativestosetuporpromoteestablishmentofdatacentresacrossthe countrytocatertogrowingneedsofArtificialIntelligence(AI)andtechcompaniesincluding the number of such centres established in past three years, State-wise, year-wise;
(b) whether Government plans for setting up more data centres in coming five to ten years byprivatesectoraswellasbyPublicSectorUndertakings(PSUs)andGovernmentbodies; and
(c) the regulations Government is going to put in place so that data of Indian citizens and Indian entities/organisations is stored in India itself and not allowed to be stored outside?

ANSWER

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

(a) to(c): Union Cabinet led by Hon'ble Prime Minister has approved the IndiaAI Mission on 7th March 2024, a strategic initiative to establish a robust and inclusive AI ecosystem that aligns with the country's development goals.

IndiaAI Mission encompasses key pillars of the Al ecosystem including, IndiaAI Compute Capacity, IndiaAI Innovation Centre, IndiaAI Datasets Platform, IndiaAI Application Development Initiative, IndiaAI FutureSkills, IndiaAI Startup Financing and Safe & Trusted AI. One of the key pillars of the IndiaAI Mission is IndiaAI Compute, which aims to deliver Compute as a Service to address India's dedicated AI computing needs across various sectors. Against targeted AI compute infrastructure of 10,000 GPUs, the mission has empanelled 14,517 GPUs.

As per an industry estimates, the Data Centre capacity in India is 854 Mega Watts (MW), Information Technology Load (IT Load) and it is expected to grow to 1,645 MW by 2026.

The policies of the Government of India are aimed at ensuring a safe, trusted and accountable cyberspace for users in the country. The key regulatory initiatives taken by the Ministry of Electronics & Information Technology (MeitY) and the other sectoral regulators to address the issues of cybersecurity measures to secure critical infrastructure and personal data protection in the cyberspace through reasonable security practices, are as under:

(i) Section 43A of the IT Act prescribes for compensation for failure to protect sensitive personal data or information of users. Anybody corporate handling sensitive personal data or information can be held liable if a user suffers a loss due to their negligence in implementing reasonable security practices.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information), 2011 ("SPDI Rules") made under section 43A of the IT Act has prescribed reasonable security practices and procedures to protect sensitive personal data of users collected by a body corporate.

The IT Act read with the SPDI Rules, provide for regulations regarding the handling, processing, and storage of sensitive personal data. However, these regulations do not explicitly mandate data localisation (i.e., the exclusive storage of data within India). Instead, they impose strict consent and security requirements for transferring sensitive data outside India.

The SPDI Rules state that a body corporate may transfer sensitive personal data or information (SPDI) to another body corporate or a person in or outside India, provided that the recipient ensures the same level of data protection as required under the SPDI Rules. Such transfer is permitted only when it is necessary for the fulfilment of a lawful contract or when the individual has provided explicit consent for the transfer. Also, section 72A of the IT Act provides for penalty for disclosure of personal information in breach of the lawful contract.

(ii) Additionally, the Digital Personal Data Protection Act, 2023 ("DPDP Act") received the assent of the Hon'ble President on August 11, 2023. The DPDP Act, which is yet to come into force, establishes a legal framework to regulate the processing, including the sharing, of digital personal data. The Act imposes obligations on Data Fiduciaries to protect digital personal data in their possession or under their control. This includes ensuring that any processing undertaken by them or on their behalf by a Data Processor complies with the Act. Data Fiduciaries are required to implement reasonable security safeguards and adopt appropriate technical and organisational measures to ensure compliance with the Act's provisions.

The Act emphasises principles such as lawful data processing, purpose limitation, and data minimisation. It also establishes the Data Protection Board of India to oversee compliance and address grievances. The DPDP Act does not explicitly mandate data localisation. Instead, it empowers the Central Government to restrict data transfers to specific countries or territories through official notifications. However, any sectoral laws that provides higher degree of protection for or restriction on transfer of personal data will continue to apply, ensuring higher protection levels where required.

(iii) Further, Reserve Bank of India (RBI) issued a directive vide circular DPSS. CO.OD. No 2785/06.08.005/2017-18 dated 6th April, 2018 on "Storage of Payment System Data" advising all system providers to ensure that, within a period of six months, the entire data

relating to payment systems operated by them is stored in a system only in India.https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF

The RBI's data storage directions under the Payment and Settlement Systems Act, 2007 apply to all Payment System Operators (PSOs) authorised by the RBI. They cover:

- Banks operating as system operators or participants in RTGS, NEFT, CCIL, NPCI, and card schemes.
- System participants, service providers, intermediaries, payment gateways, third-party vendors, and other entities engaged in the payments ecosystem.

Authorised PSOs are responsible for ensuring that payment data is stored exclusively in India, as mandated by the RBI.

As per Insurance Regulatory & Development Authority of India (IRDAI) (Maintenance of Information by the Regulated Entities and Sharing of information by the Authority), Regulations 2024, every insurer shall maintain a record of every policy issued and a record of every claim made by it in electronic form and ensure that such records shall be held in Data Centres located and maintained in India only. The said Regulations can be viewed at https://irdai.gov.in/document-detail?documentId=6540652 .

Also, the IRDAI Information and Cyber Security Guidelines provides for the requirement of storing the Business and Critical Data including the ICT logs in India. The said guidelines can be viewed at https://irdai.gov.in/document-detail?documentId=3314780 .

******