GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 6119
TO BE ANSWERED ON: 01.04.2026

ACCESS OF PRIVATE COMPANIES TO DIGITAL PUBLIC INFRASTRUCTURE

† 6119. SHRI RAJESH RANJAN:

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

(a) the number of private companies granted access to Government digital public infrastructure platforms during each of the last five years, platform-wise;
(b) the number of agreements, Memorandum of Understanding (MoU) or partnerships entered into with such companies and the reasons cited in the Ministry's review for permitting private access to digital public infrastructure;
(c) the number of complaints and representations received regarding data security, consent and misuse of digital public infrastructure by private companies, State-wise particularly for the State of Bihar;
(d) the key findings of monitoring, audit and security assessment reports relating to safeguards governing private access to public digital platforms; and
(e) the regulatory, contractual and oversight measures introduced to ensure accountability, transparency and protection of citizen's data in such partnerships?

ANSWER

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

(a) to (e): In line with Hon'ble Prime Minister's vision to democratize technology and empower citizens, the Government of India launched the Digital India programme in July 2015.

The programme focuses on expanding digital access, internet affordability, digital public infrastructure and digital literacy.

India's DPI approach
The Digital Public Infrastructure (DPI) approach is a key pillar of this programme. It enables the delivery of digital services at population scale through open, interoperable and secure platforms.

India has established an interconnected ecosystem of data and digital infrastructure platforms, integrating government platforms with startups, private enterprises, and other entities within

the DPI ecosystem. Platforms such as Aadhar, UPI, DigiLocker, etc are shining examples of the same.

This enables entities, including private ones to innovate and enhance business models, by facilitating their onboarding to such digital platforms.

Several start-ups and entities access the Digital Public Infrastructure (DPI) like Aadhaar, Unified Payments Interface (UPI), DigiLocker and other data platforms through regulated frameworks.

(i) Aadhaar stands as a cornerstone of secure, consent-driven digital identity. Through robust API-based authentication and e-KYC services, it enables real-time, trusted identity verification at scale, thereby powering seamless, paperless, and efficient service delivery across sectors. A total of 105 private Requesting Entities (RE) have been onboarded since 2021 to perform Aadhaar authentication for delivery of various user services. Further, during FY 2025-26, 71 private entities have been registered as Offline Verification Seeking Entity (OVSE) on Aadhar app.

(ii) DigiLocker has provided anytime access to authentic digital documents from original issuer for the common citizen. More than 68.11+ crore users are registered with DigiLocker to avail its services and more than 950+ crore documents issued from 2512 Issuers and 3443 Requesters onboarded on the platform.

(iii) UPI exemplifies sector-specific data access. Finance and Payments data are made available through APIs linked to the Unified Payments Interface ecosystem, thereby enabling fintech innovation at scale. This platform serves 6.5 crore merchants, and connects 694 banks on one platform, making it the world's largest digital payment system.

(iv) AIKosh under IndiaAI Mission is a sovereign AI-artefact hub offering pre-trained AI models and datasets across sectors such as agriculture, healthcare, education, governance, environment and finance. These models and other features of AIKosh can be accessed from www.aikosh.com.

(v) Open Government Data (OGD) Platform / Bharat Data Platform (data.gov.in) provides open access to government datasets under the National Data Sharing and Accessibility Policy (NDSAP). It is the largest repository of open government data in India, promoting transparency and public participation.

The platform provides about 4.54 lakh datasets and 2.36 lakh APIs, covering a wide range of sectors like agriculture, health, education, transport, energy, environment and governance.

(vi) National Data and Analytics Platform (NDAP) is a platform developed by NITI Aayog which aggregates and standardises datasets from multiple ministries into a single platform. It makes government data more comparable and accessible for researchers, startups, and policymakers to support evidence-based decisions.

It hosts around 6362 datasets across 31 sectors and 53 ministries. It provides standardized and interoperable datasets in areas such as economy, health, education, labour and infrastructure. These datasets are available for access at https://ndap.niti.gov.in.

(vii) Ayushman Bharat Digital Mission maintains health record data and enables sharing through digital health exchanges, alongside Aadhaar-based identity and authentication APIs. This forms the backbone of India's health data infrastructure by creating an integrated digital health ecosystem, rather than publishing open datasets.

While OGD provides the largest volume of open data, NDAP enhances usability through standardization, AIKosh supports AI innovation, UPI supports fintech growth and ABDM builds a secure health data infrastructure.

Together, these platforms reflect India's strategy of building open, federated, and sector-specific data infrastructure to power AI development, public service delivery, and research.

These systems enable secure, seamless, and trusted interactions among citizens, businesses, and governments. The architecture is designed to drive innovation, enhance transparency, and deliver efficient, citizen-centric public services through open, regulated, and sector-specific access frameworks.

Indian legal and regulatory frameworks also exist to prevent its misuse in this regard include Digital Personal Data Protection Act 2023, Information Technology Act 2000 and sector-specific guidelines from regulators like UIDAI, RBI, etc.

Complaints related to unauthorized access to personal data, fraudulent financial transactions and data scraping are handled by sector regulators (e.g., banking, telecom), National Cybercrime Reporting Portal (cybercrime.gov.in), CERT-In and platform-specific grievance systems.

Comprehensive security audit has been done for the data.gov.in portal. UIDAI also conducts periodic audits of its systems.

UIDAI has implemented a three-tier audit framework, comprising the Self-Compliance Audit, the Information Security Annual Audit, and the GRCP (Governance, Risk, Compliance, and Privacy) Audit, for entities in the Aadhaar Authentication Ecosystem.

Similarly, internal reviews and security audits are conducted by other concerned organizations like banks and Ministries/Departments. These audits periodically examine issues relating to consent architecture, data retention and security safeguards, and necessary improvements are subsequently undertaken to fill the gaps.

The different types of penalties include financial penalties for data misuse, suspension of API access, revocation of platform licenses and criminal penalties in severe cases. For example, the DPDP Act introduces significant financial penalties for data breaches or non-compliance.

The safeguards consist of mandatory user consent, purpose limitation (data used only for stated purpose), data minimisation, security safeguards and encryption and independent audits.

****