BACKGROUNDERS
Press Information Bureau
Government of India

International Data Privacy Day

Strengthening confidence in India's evolving digital ecosystem

27 January 2026

Key Takeaways

- **Data Privacy Day** highlights the shared responsibility of the government, digital platforms, and citizens in building a secure and trusted digital ecosystem.
- India is the world's **3rd-largest digitalised economy**, with digital platforms embedded in daily economic and social life.
- The **DPDP Act, 2023 and DPDP Rules, 2025** provide a citizen centric framework balancing data privacy, innovation, and public interest.
- **₹782 crore** allocated in the budget **2025–26** for cybersecurity to safeguard digital public infrastructure.

Introduction

Data Privacy Day is internationally observed annually on 28 January. It aims to raise awareness about the importance of protecting personal data and privacy in the digital age. Also known as **Data Protection Day**, it was designated in 2006 by the Council of Europe to commemorate the signing of Convention 108- the world's first legally binding international treaty on data protection.

Data privacy is a foundational pillar of responsible digital governance. It protects and safeguards citizens' personal information across large-scale digital public platforms. Data privacy builds public trust by strengthening confidence in government-led digital services. Robust data privacy frameworks enable responsible digital use by promoting the safe, ethical, and secure adoption of digital technologies. They also help reduce data and cyber risks by preventing misuse, mitigating cyber threats, and identifying data-related frauds. Furthermore, strong data-protection regimes enhance governance and accountability by ensuring transparency, effective oversight, and clearly defined institutional responsibilities.

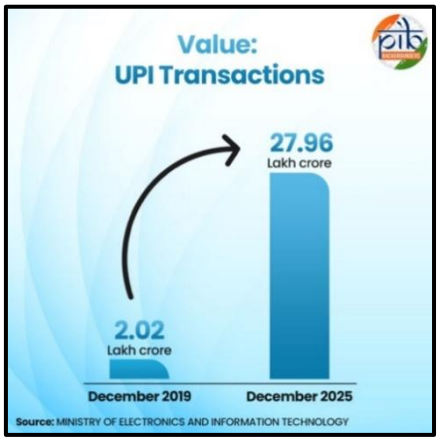
In an increasingly digital society, safeguarding personal data is essential to sustaining trust, security, and inclusion. As digital public platforms expand in scale and impact, a strong commitment to data privacy ensures that innovation remains citizen centric, ethical, and accountable. Observing Data Privacy Day reinforces the collective responsibility of governments, institutions, and citizens in protecting digital rights.

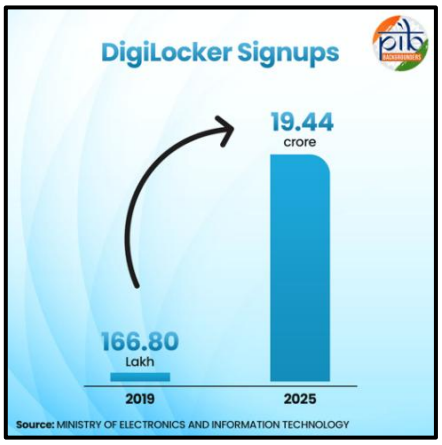
India's Expanding Digital Footprint and the Privacy Imperative

India's rapid digitalisation has transformed the way citizens interact with the State, access services, and participate in governance. Digital platforms now operate at population scale, making data a critical public resource that underpins service delivery, inclusion, and innovation. While this transformation has delivered efficiency and accessibility, it has also heightened the importance of safeguarding personal

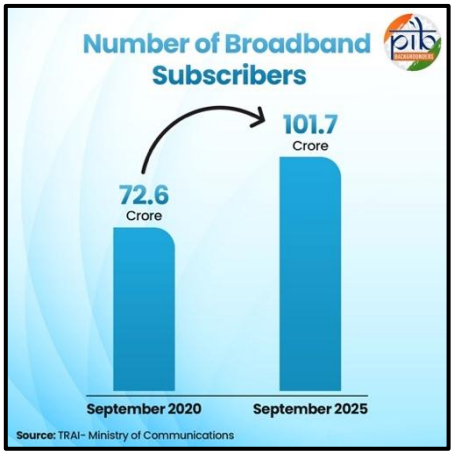
data. As India's digital footprint continues to expand, embedding privacy and security into digital systems has become a central governance priority.

1. **Scale and Reach of India's Digital Public Infrastructure:** India's Digital Public Infrastructure (DPI) has emerged as the backbone of its digital transformation, enabling seamless delivery of services and large-scale citizen participation. Flagship initiatives such as **Aadhaar** have established a trusted digital identity framework, while **UPI** has revolutionised everyday financial transactions through real-time digital payments. Platforms supporting paperless governance have streamlined public service delivery, and citizen centric platforms such as **MyGov, with over 6 crore users, have strengthened participatory governance**, while **eSanjeevani has facilitated more than 44 crore digital health consultations**, significantly expanding access to healthcare. Together, these initiatives demonstrate the scale, depth, and inclusiveness of India's DPI, while also reinforcing the need for strong data protection and privacy safeguards to sustain trust at scale.





2. **Connectivity, Affordability and Digital Inclusion at Population Scale:** India's digital scale is reinforced by its position as the world's third-largest digitalised economy, supported by over **101.7 crore broadband subscribers (as of Sept 2025)**, each spending an average of **1,000 minutes online**. Affordable connectivity, at **$0.10 per GB (2025) of mobile data**, has further accelerated adoption, positioning India among the most connected and digitally inclusive societies globally. Today, digital platforms touch core aspects of daily life, including identity verification, payments, healthcare delivery, education, grievance redressal, and citizen participation, making digital access a defining feature of India's socio-economic landscape.



3. **Strengthening Privacy and Cybersecurity:** The scale that powers inclusion and efficiency also intensifies the **privacy and the cybersecurity imperative**. The exponential growth in digital interactions has led to a surge in the volume and sensitivity of personal data being generated, processed, and stored, increasing exposure to risks such as data misuse, cyber threats, and privacy breaches. Recognising this, the Government has strengthened institutional safeguards through enhanced data protection and cybersecurity frameworks, including an allocation of **₹782 crore for cybersecurity projects** (2025–26).

The observance of **International Data Privacy Day on 28 January** reinforces India's commitment to responsible data practices, public awareness, and trust-based digital governance. As India's digital platforms continue to expand in scale and complexity, embedding **privacy by design, robust oversight,**

and institutional accountability will remain central to ensuring that digital innovation remains secure, inclusive, and citizen centric.

National Data Privacy & Security Readiness

As digital technologies increasingly underpin governance, service delivery, and economic activity, ensuring robust data privacy and cybersecurity has become a national priority. India's expanding digital ecosystem requires a strong legal and institutional framework that protects personal data, secures digital transactions, and builds trust among citizens and businesses. In response, India has put in place a comprehensive and evolving regulatory architecture that balances privacy protection with innovation, accountability, and ease of compliance.

Information Technology (IT) Act, 2000

The **IT Act, 2000** is India's core law for cyberspace, providing the legal basis for **e-governance, digital commerce, and cybersecurity**. In alignment with the National Data Protection and Cybersecurity objectives, the Act grants legal recognition to **electronic records and digital signatures**, enabling secure online transactions and digital delivery of public services. The Act also establishes key **cybersecurity and regulatory mechanisms**, including **CERT-In** as the national incident response agency, along with adjudicatory and appellate bodies for cyber disputes. Provisions such as **Sections 3, 3A, 6, 46, 69A, and 70B** collectively support authentication, e-governance, adjudication, content blocking for national security, and cyber incident management, forming a robust and secure digital framework for India.

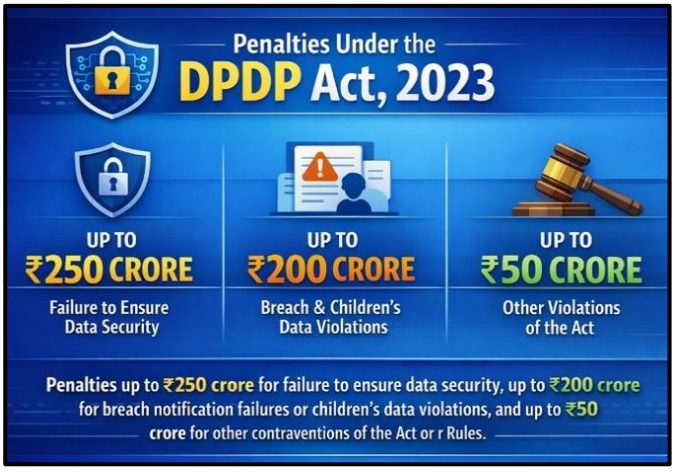
Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, notified under the Information Technology Act, have been formulated in line with India's evolving data security and cybersecurity requirements. The Rules lay down due diligence requirements for intermediaries to ensure a safe, trusted, and transparent online environment. Under the Rules, all intermediaries are mandated to establish a robust grievance redressal mechanism for addressing complaints from users or victims in a time-bound manner.

- **Intermediaries** are defined as entities that store or transmit data on behalf of others, include telecom and internet service providers, online marketplaces, search engines, and social media platforms.

Digital Personal Data Protection (DPDP) Act, 2023

The **DPDP Act, 2023, enacted on 11 August 2023**, governs the processing of personal data collected through digital means, including data digitised from offline sources. The Act seeks to strike a careful balance between protecting individual privacy and enabling lawful data use to support innovation, service delivery, and economic growth. It follows a **SARAL approach: Simple, Accessible, Rational, and Actionable**, to ensure clarity, ease of understanding, and practical compliance for all stakeholders.



Data Protection Board of India: A key institutional feature of the Act is the establishment of the **Data Protection Board of India**, which is responsible for overseeing compliance, conducting inquiries into data breaches, and ensuring timely corrective action. The Board plays a central role in enforcing the provisions

of the Act and in strengthening public trust by providing an effective, accountable mechanism for redressal and enforcement.

At its core, the DPDP Act empowers citizens as Data Principals, placing individuals at the centre of India's data protection framework by granting them clear rights, greater control over their personal data, and assurance that organisations handling such data remain responsible, transparent, and accountable.

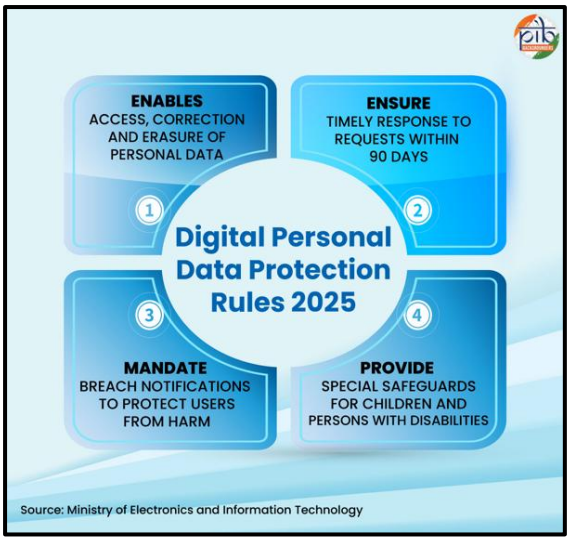
Rights and Protections for citizens under DPDP Act, 2023			
Right to Give or Refuse Consent: Individual has a choice to allow or deny the use of their personal data.	**Right to Know How Data is Used:** Individuals can seek information on what personal data has been collected, why it has been collected and how it is being used.	**Right to Access Personal Data:** Individuals can ask for a summary of their personal data processed that is done by a Data Fiduciary.	**Right to Correct Personal Data:** Individuals may request corrections to personal data that is inaccurate or incomplete.
Right to Update Personal Data: Individuals can ask for changes when their details have altered, such as a new address or updated contact number.	**Right to Erase Personal Data:** Individuals may request the erasure of personal data in certain situations. The Data Fiduciary must consider and act on this request.	**Right to Nominate Another Person:** Every individual can appoint someone to exercise their data rights on their behalf in case of her death or incapacity.	**Mandatory Response within Ninety Days:** Data Fiduciaries are required to address all requests related to access, correction, updating or erasure within a maximum of ninety days, ensuring timely action and accountability.
Protection During Personal Data Breaches: If a breach takes place, individuals must be informed at the earliest. The message must explain what happened and what steps individual can take.	**Clear Contact for Queries and Complaints:** Data Fiduciaries must provide a point of contact for questions relating to personal data. This may be a designated officer or a Data Protection Officer.	**Special Protection for Children:** When a child's personal data is involved, verifiable consent from a parent or guardian is required. This consent is needed unless the processing relates to essential services such as healthcare, education or real-time safety.	**Special Protection for Persons with Disabilities:** If an individual with a disability cannot make legal decisions even with support, her lawful guardian is required to give consent. This guardian must be verified under the relevant laws.

- **Data Fiduciary:** An entity that decides why and how personal data is processed, either alone or with others.
- **Data Principal:** The individual to whom the personal data relates. In the case of a child, this includes a parent or lawful guardian. For individuals with a disability who cannot act independently, this includes the lawful guardian acting on their behalf.

Digital Personal Data Protection Rules, 2025

Notified on **13 November 2025**, the **Digital Personal Data Protection Rules, 2025** operationalise the **DPDP Act, 2023**, strengthening India's data protection framework. Altogether, they establish a **clear, citizen centric regime** that safeguards personal data while enabling innovation and responsible use.

The Rules place individuals at the centre by **empowering citizens with enforceable rights**, enhancing accountability of organisations, and curbing misuse and unauthorised exploitation of data.



Together, the **DPDP Act and Rules** provide regulatory clarity and balance privacy with innovation, supporting a **secure, transparent, and future-ready digital economy**.

Altogether, these frameworks constitute a coherent and forward-looking approach to data governance in India. By clearly defining rights, responsibilities, and enforcement mechanisms, these measures strengthen institutional accountability, empower citizens, and foster trust in digital systems. As India's digital economy continues to grow in scale and complexity, this robust legal and regulatory foundation ensures that data-driven innovation remains secure, transparent, and citizen centric, reinforcing India's readiness for a resilient and future-ready digital ecosystem.

Additional National Measures for Data Security

The Government of India has undertaken multiple initiatives to strengthen cybersecurity standards, reinforce digital infrastructure, and promote cyber awareness, with the objective of ensuring an open, safe, trusted, and accountable Internet ecosystem. In view of evolving cyber threats, the following measures have been implemented:

1. **Incident Prevention, Response, and Security Management** **IT Act, 2000, establishes CERT-In** as a nodal agency responsible for cybersecurity, with a vision of proactively securing India's cyberspace, and to enhance the security of India's Communications and Information Infrastructure through proactive measures and effective collaboration.

2. **National Coordination for Cyber and Data Security** The **Indian Cyber Crime Coordination Centre (I4C)** approved in October 2018, established by the Ministry of Home Affairs, serves as the national nodal agency to **prevent, detect, and respond to cybercrime**, with a special focus on crimes against women and children, supported by early warning systems and trend analysis. It also facilitates easy cybercrime reporting, builds public awareness, and strengthens the capacity of States/UTs through training of law enforcement, prosecutors, and judicial officers in cyber forensics, investigation, and cyber hygiene.

3. **Citizen centric Data Protection and Fraud Response Systems** Platforms such as the **National Cyber Crime Reporting Portal (NCRP)** operational from January 2020 and the **Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS)** enable timely reporting of cyber incidents and financial frauds, supported by the nationwide helpline **1930**, helping safeguard personal and financial data at scale.

4. **Real-Time Interventions** A dedicated **Cyber Fraud Mitigation Centre (CFMC)** launched in September 2024 **facilitates real-time data sharing** and coordinated response among banks, financial institutions, telecom service providers, and Law Enforcement Agencies, enabling rapid blocking of compromised accounts, SIM cards, and devices used in cyber-enabled fraud.

5. **Digital Infrastructure Protection and Enforcement Tools** The Government has strengthened enforcement through digital platforms such as **Sahyog** for expedited takedown of unlawful online content, and the **Suspect Registry**, developed in collaboration with financial institutions, to identify and disrupt mule accounts and fraud-linked digital identifiers. Additionally, Indigenous cybersecurity tools are being developed by the **Centre for Development of Advanced Computing (C-DAC)** to strengthen self-reliance and reduce dependence on foreign security solutions.

6. **Cyber Forensics and Investigation: National Cyber Forensic Laboratories** provide specialised forensic and investigative support to States/UTs, enhancing national capacity for data breach analysis, evidence preservation, and cyber incident prosecution.

7. **Data-Driven Analytics** The **Samanvaya Platform** launched in September 2024, functions as a national Management Information System and analytics system for cybercrime data, enabling inter-State coordination, crime pattern analysis, and geo-mapping of cybercrime infrastructure to support data-informed enforcement actions.

8. **Human and Institutional Capabilities** Capacity-building efforts such as the **CyTrain digital learning platform launched in March 2019** and the **Cyber Commando Programme launched in September 2024** are strengthening a skilled cybersecurity workforce, complemented by the Information Security Education & Awareness (ISEA) programme and its dedicated portal (www.infosecawareness.in), while the Certified Security Professional in Artificial Intelligence (CSPAI) programme launched by CERT-In in September 2024 equips professionals to secure AI systems and address emerging AI-related cyber threats.

9. **National Awareness Campaigning** The **Cyber Swachhta Kendra (CSK)**, a citizen-focused initiative of CERT-In, functions as a **Botnet Cleaning and Malware Analysis Centre**. It provides free tools for malware detection and removal, disseminates cybersecurity best practices, and issues daily alerts on botnet and malware infections along with remedial measures to organisations across sectors.

These initiatives reflect the Government of India's comprehensive and forward-looking approach to cybersecurity, combining standards, capacity building, citizen awareness, and crisis preparedness. By strengthening institutional mechanisms and aligning with global best practices, India continues to enhance trust, resilience, and security across its digital ecosystem in the face of evolving cyber threats.

Conclusion

Data Privacy Day serves as a timely reminder that trust is the cornerstone of India's rapidly expanding digital ecosystem. As digital public infrastructure increasingly shapes governance, service delivery, and everyday life across the country, protecting personal data is not merely a technical requirement but a democratic imperative. India's evolving legal frameworks, strong institutional mechanisms, and citizen centric initiatives reflect a firm commitment to ensuring that digital innovation remains safe, ethical, and accountable.

With the rollout of the Digital Personal Data Protection Framework, strengthened cybersecurity institutions, and sustained investments in capacity building and awareness, India is steadily advancing towards a secure and future-ready digital environment. Recognising the significance of data privacy reinforces the shared responsibility of the Government, digital platforms, and citizens to safeguard personal data, build trust, and ensure that India's digital transformation remains inclusive, resilient, and citizen centric.

References

Ministry of Communications

- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2088195&reg=3&lang=2
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2143158&reg=3&lang=2
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2198285&reg=3&lang=1
- https://www.pib.gov.in/PressReleseDetail.aspx?PRID=2206477&reg=3&lang=1
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2057035&reg=3&lang=2

Ministry of Electronics & Information Technology

- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2181719&reg=3&lang=2
- https://eparlib.sansad.in/bitstream/123456789/2998224/1/AU1649_oHDiWm.pdf

- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2116341&reg=3&lang=1
- https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf

Ministry of Home Affairs

- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2205201&reg=3&lang=2

PIB Headquarters

- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190655&reg=3&lang=2
- https://www.pib.gov.in/PressReleseDetail.aspx?PRID=2197871&reg=3&lang=2
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146&reg=3&lang=2
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2198260&reg=3&lang=1

Data Protection Day, EU

- https://data-protection-day.eu/

Data Protection Day, Council of Europe

- https://www.coe.int/en/web/data-protection/data-protection-day

Others

- https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

PIB Research