INDIALAW

CIVIL

# India Moves Closer to Enforcing Data Protection Law: MeitY Completes Review of Public Feedback

AUTHOR Aditi Rana, Rahul Sundaram

PUBLISHED 29 July 2025

## Introduction: MeitY Signals Readiness to Operationalise India's Data Protection and Cybersecurity Framework

On July 28, 2025, the Ministry of Electronics and Information Technology (MeitY) issued an official update regarding the status of two major regulatory initiatives: the Digital Personal Data Protection Rules, 2025 and India's National Cybersecurity Strategy. The update confirms that MeitY has concluded the public consultation process for the draft rules under the Digital Personal Data Protection Act, 2023 (DPDP Act), having received 6,915 responses, and is in the process of finalising the regulatory framework to bring the law into effect.

This development is significant as it marks India's transition from legislative intent to enforceable obligations in the areas of data privacy and cybersecurity governance.

## Background: The Road to Implementation

The DPDP Act, 2023, enacted in August 2023, provides the statutory framework for lawful processing of digital personal data in India. While the Act has been notified, its provisions are not yet in force. On January 3, 2025, MeitY released the Draft Digital Personal Data Protection Rules, 2025 for public consultation. The July 28 update confirms that the feedback phase has concluded and that the Ministry is now reviewing the submissions to finalise the rules.

## Key Takeaways from the July 28, 2025 MeitY Update

1. **Public Consultation on Draft Rules Concluded**

MeitY confirmed that it received 6,915 responses to the Draft Digital Personal Data Protection Rules, 2025, from a wide spectrum of stakeholders including industry, academia, civil society, and individuals. These responses are under detailed examination and will inform the finalisation of the rules.

2. **Enforcement of DPDP Act Linked to Rule Notification**

The update reiterates that the DPDP Act, 2023 will be brought into force only after the final rules are notified. MeitY is currently developing standardised formats for privacy notices, consent mechanisms, and breach reporting. It is also preparing to establish the Data Protection Board of India, which will play a key role in implementation and enforcement.

3. **National Cybersecurity Strategy**

MeitY is actively developing a comprehensive National Cybersecurity Strategy aimed at enhancing national cyber resilience. It will focus on strengthening key institutions including CERT-In (under Section 70B of the IT Act, 2000), National Critical Information Infrastructure Protection Centre (NCIIPC), and the National Cyber Security Coordinator.

4. **Cyber Awareness and Capacity-Building Initiatives**

The update outlines a range of initiatives undertaken to build public awareness and institutional capability. These include:

- Observance of Cybersecurity Awareness Month and Safer Internet Day;
- Multilingual outreach through regional language campaigns;
- The CyberShakti initiative, which promotes women's participation in cybersecurity; and
- The ISEA Programme, which has trained over 8 lakh individuals through 3,600+ workshops.

5. **Tools and Portals for Citizen Cyber Hygiene**

MeitY highlights public-facing tools such as the Cyber Swachhta Kendra (CSK), which offers malware cleaning utilities and promotes safe computing practices. Citizens are also directed to www.safeonline.in, maintained by CERT-In, for guidance on cyber hygiene and incident reporting.

6. **Continuity of Existing Security Obligations**

Until the DPDP Act is notified, the existing Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 continue to govern data security obligations. These remain in force and are supported by the institutional ecosystem referenced in the update.

## Implications for Businesses and Digital Entities

The July 28 update is an inflection point for the compliance landscape in India. It provides regulatory certainty that:

- The rules will be notified soon, and the DPDP Act will come into force thereafter;
- Entities processing personal data will soon be subject to enforceable compliance obligations;
- Breach reporting, DPO appointments, data retention policies, and cross-border data transfer governance will become legally binding;
- Enforcement mechanisms through the Data Protection Board of India will be activated, with potential penalties up to ?250 crore per instance of non-compliance.

Businesses operating in sectors such as e-commerce, financial services, ad-tech, healthcare, social media, and ed-tech, especially those engaging in profiling or cross-border processing should prioritise internal readiness.

## Conclusion

MeitY's July 2025 update is a clear indication that India is entering the implementation phase of its personal data protection and cybersecurity law framework. Once the final rules are notified, the DPDP Act will move from a legislative instrument to an enforceable statute, bringing with it a structured compliance ecosystem.

Entities that rely on digital personal data, whether of consumers, employees, or business partners must act swiftly to align with the upcoming requirements. This includes reviewing internal data flows, updating privacy notices and policies, implementing breach response protocols, and ensuring board-level visibility of data governance.

For more details, write to us at: contact@indialaw.in

## Related Practice Areas

**Data Protection and Privacy**