June 2025

Ministry of Electronics and Information Technology releases blueprint for consent management

As India moves toward implementing the Digital Personal Data Protection Act, 2023 ("**DPDP Act**"), a key focus area has been developing robust frameworks for user consent management. In this context, the National e-Governance Division under the Ministry of Electronics and Information Technology ("**MeitY**"), has published a Business Requirement Document ("**BRD**") for consent management.

The BRD is a non-binding technical reference issued by MeitY's Startup Hub and is not part of the DPDP Act. The BRD was published as part of an Innovation Challenge, inviting participants to build a prototype Consent Management System ("**CMS**"). It is accessible on the MeitY Startup Hub website *here*. While the document is not intended to serve as official guidance under the DPDP Act, it does, however, serve as an early indication of how the government may be thinking about consent architecture.

Regulatory context

The DPDP Act is not currently enforceable. The Government released the Draft Digital Personal Data Protection Rules, 2025, in January 2025, to operationalise the law. These draft rules address procedures and technical standards for compliance, including obligations around security, notices, and breach notifications. The public consultation period closed in March 2025, and final rules are awaited.

Key features of the BRD

The BRD lays out a modular, privacy-by-design CMS architecture, supporting the full consent lifecycle - collection, validation, renewal, withdrawal, and auditing. Some of the notable features include:

Consent collection

Consent is triggered when an individual initiates a service requiring personal data processing, such as account registration or onboarding. The CMS identifies the relevant processing purposes and generates consent requests accordingly. In this context:

1. consent must be unbundled, granular, and purpose-specific, collected *via* explicit UI controls (e.g., toggles, checkboxes), with no pre-checked options;
2. consent must be validated as free, specific, informed, unambiguous, explicit, and affirmatively given;
3. upon validation, the CMS generates a consent artefact containing key metadata (user ID, purpose ID, session ID, timestamp, consent method), which is securely stored in the consent database;

4. the system synchronises consent status across internal and external processors in real time via application programming interfaces; and
5. users receive an acknowledgement notification confirming submission, and all events are logged for auditability.

Consent validation

Before any data processing activity occurs, the CMS must validate the consent whether the required consent exists and remains active. Consent may be validated in the following manner:

1. when a data controller initiates a processing action or system query, the CMS checks its database for an active consent artefact matching the specified purpose and user ID;
2. consent must be current and not withdrawn or expired;
3. importantly, processing must remain within the scope of the consent provided. For instance, personal data collected for authentication cannot be reused for marketing without separate consent;
4. based on the outcome, the CMS either approves or denies processing. The user is notified of any denial; and
5. all validation actions are immutably logged to maintain a verifiable audit trail.

Cookie consent

1. The cookie consent component ensures transparency and control over tracking technologies used on websites and apps, empowering users to make informed choices about their data.
2. On the first visit, a cookie banner must inform users of the use of cookies and similar technologies.
3. Users must be provided granular consent options across cookie categories such as essential, performance, analytics, and marketing.
4. Only essential cookies may be enabled by default; all others require explicit, opt-in consent.
5. The CMS must offer a dedicated cookie preference interface where users can modify or withdraw consent at any time, with preferences updated in real time.

Grievance redressal

The BRD outlines a comprehensive redressal system as described below, that allows individuals to raise complaints related to data processing, privacy violations, or consent issues:

1. complaints will be automatically categorised (e.g., consent violation, data breach, processing error) and assigned unique reference IDs;
2. acknowledgement notifications will be sent upon submission, and all complaint data (user ID, timestamp, complaint type, and description) will be securely transmitted using TLS 1.3 (one point three) encryption;
3. a real-time resolution tracking dashboard will display complaint status (e.g., submitted, in progress, resolved), with updates and outcome notifications issued to the user; and
4. an escalation workflow will auto-forward unresolved complaints to the data protection officer if not closed within specified timeframes.

Conclusion

The BRD offers a preview of the operational contours of consent management under India's evolving data protection regime. While non-binding, it can help organisations future-proof their systems and prepare for robust, compliant consent workflows.

Infotech Practice

Our team understands the importance of data privacy in today's digitally interconnected world. We have dedicated our practice to ensuring that your and your customers' personal and business data remains secure, compliant, and respects the sovereignty of individuals and jurisdictions globally.

We prioritise creating bespoke solutions tailored to your business needs. We recognise that every business has unique data privacy challenges, and we use our deep understanding of international and domestic regulations to provide you with the most effective and robust legal strategies. JSA provides advice on highly sophisticated data management, data security and privacy issues. Our depth of experience gives our clients the crucial advantage of consistent and comprehensive, yet practical advice. Our Technology Law Practice group has successfully worked with several multinational organisations for the structuring and roll-out of privacy and information-security programs. We have carried out audit and risk assessments, customised global privacy and information management policies, helped create international data transfer strategies, structure and negotiate complex international data transfer agreements.

This Prism has been prepared by:

Probir Roy Choudhary
Partner

Yajas Setlur
Partner

Shivani Bhatnagar
Senior Associate

18 Practices and
41 Ranked Lawyers

7 Ranked Practices,
21 Ranked Lawyers

14 Practices and
12 Ranked Lawyers

12 Practices and 50 Ranked Lawyers

20 Practices and
22 Ranked Lawyers

8 Practices and
10 Ranked Lawyers
Highly Recommended in 5 Cities

Recognised in World's 100 best competition practices of 2025

Among Best Overall
Law Firms in India and
14 Ranked Practices

---

9 winning Deals in
IBLJ Deals of the Year

---

11 A List Lawyers in
IBLJ A-List - 2025

Asia M&A Ranking 2024 – Tier 1

Employer of Choice 2024

Energy and Resources Law Firm of the Year 2024

Litigation Law Firm
of the Year 2024

Innovative Technologies Law Firm of the Year 2023

Banking & Financial Services
Law Firm of the Year 2022

Ranked Among Top 5 Law Firms in India for ESG Practice

2022

Ranked #1
Best Law Firms to Work

Top 10 Best Law Firms for Women

For more details, please contact km@jsalaw.com

jsa
advocates & solicitors

Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi