Lakshmikumaran Sridharan attorneys
SINCE 1985
exceeding expectations

APRIL 2025 / Issue-1

TechnoLAWgy

A Technology Law Bulletin

Lakshmikumaran & Sridharan Attorneys

Table of Contents

Role of Consent Managers: Insights from the Draft Digital Personal Data Protection Rules

By **Aryashree Kunhambu**

India's data protection landscape has long positioned 'consent' as a cornerstone of lawful data processing, and the Digital Personal Data Protection Act, 2023 ('**Act**') continues to place consent as a primary legal basis for processing digital personal data. However, the Act elevates the threshold for obtaining valid consent by embedding the principles of *transparency*, *accountability* and *individual autonomy* by requiring it to be free, specific, informed, unambiguous and affirmative consent.[1]

Recognizing the operational and compliance challenges inherent in managing consent at scale by Data Fiduciaries[2], the Act introduces '**Consent Managers**'[3] to serve as an independent platform that facilitates the giving, management, review and withdrawal of consent by Data Principals.[4]

In this article, we explore the defined role, responsibilities and operational contours of a Consent Manager as provided in the recently released draft Digital Personal Data Protection Rules, 2025 ('**Draft Rules**').

Eligibility criteria for registration as a Consent Manager

Under the Act, any entity seeking to function as a Consent Manager is required to be registered with the Data Protection Board of India[5] ('**DPB**'). The Draft Rules specify a detailed set of technical, operational and financial criteria that an applicant must fulfill to be eligible for such registration. These requirements are designed to ensure that a Consent Manager possesses the requisite institutional capacity, governance standards and technical capabilities to effectively discharge its obligations under the Act.

Some of the key requirements include:

- Incorporation as a company in India, demonstrating sound financial position and competent management;
- Possessing adequate technical, operational and financial capacity to perform Consent Manager functions effectively;

[1] Section 6(1) of the Act.

[2] Section 2(i) of the Act provides that, the term 'Data Fiduciary' means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

[3] Section 2(g) of the Act provides that, the term 'Consent Manager' means a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform.

[4] Section 2(j) of the Act provides that, the term 'Data Principal' means the individual to whom the personal data relates and where such individual is— (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful guardian, acting on her behalf.

[5] Section 18 of the Act.

- Maintaining a minimum net worth of INR 2,00,00,000 (*rupees two crore*);
- Express provisions for adherence to conflict-of-interest obligations and any amendments thereto (with prior approval from the DPB) in its memorandum and articles of association;
- Aligning its operational objectives with the interests and rights of Data Principals; and
- Have its platform independently certified for compliance with such standards, as specified by the DPB.

Obligations and functions of a Consent Manager

The Draft Rules set out a detailed regulatory framework governing the role and obligations of Consent Managers, whereby a Consent Manager is envisaged not merely as an intermediary for consent collection but as a pivotal entity responsible for enabling secure, transparent and user-centric consent management. Specifically, it must operate an interoperable digital platform—accessible through a website or mobile application—that performs the dual functions of: (a) enabling a Data Principal to give, manage, review and withdraw her consent based on the privacy notice or other relevant information provided to her; and (b) allowing the Data Fiduciary to rely on such consent to lawfully deliver its goods or services to such Data Principal.

Further, a Consent Manager is directly accountable to the Data Principal and is expected to act on her behalf as per the conditions prescribed under the Draft Rules. To this end, the Draft Rules impose specific operational constraints. Firstly, the Consent Manager must remain 'data blind,' implying that it should ensure that personal data underlying the consent is not accessible or readable by the Consent Manager. Secondly, it is prohibited from subcontracting or assigning any of its obligations under the Act to third parties. Third, the Consent Manager must maintain institutional independence from Data Fiduciaries, including in respect of its directors, promoters and key managerial personnel.

In addition to the above, the Draft Rules also prescribe other ongoing obligations for Consent Managers, such as:

- Maintaining detailed records of consents obtained, notices associated with those consents, and all data-sharing activities conducted through their platforms;
- Providing Data Principals with access to their consent records and, upon request, in a machine-readable format;
- Retaining all relevant records for a minimum period of seven (7) years;
- Publishing on the digital platform relevant corporate disclosures, such as company ownership and shareholding structure;
- Maintain audit mechanisms to assess compliance with the Act and Draft Rules and periodically submit such audit reports to the DPB; and
- Seeking prior approval from the DPB before any transfer of control of the company through sale, merger, or other restructuring process.

Conclusion

In response to stringent regulations such as the European Union's General Data Protection Regulation, a global ecosystem of technology service providers has emerged to support Data Fiduciaries in managing the consent required for lawful data processing. Notably, India's DPDP Act distinguishes itself as the first legislative framework to formally institutionalize the role of a Consent Manager within its regulatory architecture. By providing an option to onboard a Consent Manager, the Act and the Draft Rules aim to reduce the operational burden of Data Fiduciaries while enhancing transparency and user agency for Data Principals.

However, the success of this model will depend upon various factors, including demand-side pressures, revenue models and the extent of acceptance by Data Principals.

Nonetheless, this model opens a spectrum of business opportunities in India, especially for entities engaged in offering data privacy and cybersecurity solutions (*such as consent orchestration*), who may be well-positioned to undertake this role. It will be critical to watch regulatory responses as well as evolving business models in this context, with the notification of the Rules.

[The author is an Associate in Technology Law practice at Lakshmikumaran & Sridharan Attorneys, Hyderabad]

Information Technology Updates

Tamil Nadu's Real Money Gaming Regulations challenged

In February 2025, the Tamil Nadu Government introduced the Tamil Nadu Online Gaming Authority (Real Money Games) Regulations ('**2025 Regulations**') in response to concerns about the social risks associated with real-money gaming ('**RMG**'). Some of the key provisions therein include:

a) A ban on individuals under 18 years of age from accessing RMG platforms;
b) Mandatory KYC verification, including Aadhaar authentication, at account creation;
c) Pop-up messages displaying time spent on the platform every hour and after every 30 minutes of gameplay;
d) A prohibition on access to RMG platforms from 12:00 AM to 5:00 AM;
e) Mandatory tools for players to set spending limits and receive real-time alerts;
f) Warning labels, such as 'online gaming is addictive,' to be prominently displayed on the RMG platforms.

The 2025 Regulations, among other laws, were challenged subsequently in a writ petition filed in the Madras High Court. The same is currently pending before the High Court.

IT Blocking Rules – Constitutional validity challenged

The Supreme Court of India has issued a notice to the Union of India in response to a writ petition filed by the Software Freedom Law Centre challenging the constitutional validity of the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 ('**IT Blocking Rules**'). The petition specifically requests the quashing of Rule 16 (*which imposes secrecy obligations*) and reading or striking down of Rules 8 and 9 (*that make it optional to issue a blocking request notice to an information originator*). According to the petitioner, the provisions violate the information originator's right to a fair hearing prior to the takedown of their content.

Karnataka High Court to hear X's petition challenging the Government's misuse of the Sahyog Portal and Section 79(3)(b) of the IT Act

X (*formerly Twitter*) has filed a writ petition before the Karnataka High Court, challenging the Government's use of Section 79(3)(b) of the Information Technology Act, 2000 ('**IT Act**') to establish a parallel content-blocking process. Section 79(3) qualifies that the immunity granted to intermediaries will not apply if they fail to remove unlawful content after being notified by

appropriate Government agencies. It is argued that this process, including the Sahyog Portal, runs parallel to the blocking powers under Section 69Aof the IT Act and does not import or consider the safeguards present thereunder

CERT-IN's Advisory on usage of Gen-AI Tools

CERT-In has published an advisory dated 26 March 2025, on 'Best Practices against Vulnerabilities while using Generative AI Solutions', identifying key threats and best practices in relation to the use of Gen-AI tools. As part of the same, it outlined the risks such as data poisoning and adversarial attacks (*where AI models are manipulated by deceptive inputs*), model inversion (*which may lead to the unauthorized exposure of sensitive training data*), and prompt injection attacks (*that could undermine the intended results of GenAI applications*). In addition to the same, the Advisory also recommends certain security measures, including robust testing, identity and access management tools, secure APIs and other measures. Organizations are also encouraged to engage in ongoing monitoring, integrating AI risk assessments within broader cybersecurity strategies, and providing training to users on the responsible use of GenAI tools.

Data Protection

On 3 January 2025, the Ministry of Electronics and Information Technology (**MEITY**') released the draft Digital Personal Data Protection Rules, 2025 ('**Draft Rules**'), aimed at operationalizing the provisions of the Digital Personal Data Protection Act, 2023. We have prepared a brief on the Draft Rules, available here.

The consultation period, initially set for 18 February and extended thereafter, concluded on 5 March 2025. The Ministry is reportedly expected to finalize the Draft Rules shortly.

Tech-Regulatory Landscape

SEBI's Rules for Registered Intermediaries

The Securities and Exchange Board of India ('**SEBI**') has issued an Advisory dated 21 March to curb the rise in fraud related to the securities market on social media platforms by 30 April 2025. To this end, it issued the Advisory requiring SEBI-registered intermediaries to update their mobile numbers and email addresses on the SEBI Intermediary Portal and use only such emails and mobile numbers should they wish to advertise on such platforms. It also provides that the providers of such platforms would conduct advertiser verification thereafter against the details furnished on the SEBI Intermediary Portal and may upload or publish advertisements thereafter.

RBI imposes penalty for non-compliance with P2P Directions

The Reserve Bank of India ('**RBI**') has, *vide* orders dated 7 March 2025, imposed penalty on four companies *viz.* Faircent, Finzy, Visionary, and Rang De, for non-compliance with the Master Directions – Non-Banking Financial Company – Peer to Peer Lending Platform (Reserve Bank) Directions, 2017, including assuming partial credit risks, breaching fund transfer mechanisms, and lack of policy implementation.

Telecom Commercial Communications Customer Preference Regulations amended

The Telecom Regulatory Authority of India ('**TRAI**') amended the Telecom Commercial Communications Customer Preference Regulations 2018 '**TCCCPR**'). The amendments now enable lodging of spam complaints within seven days and resolution of complaints against unregistered senders within five days. Additionally, the amendments also include an opt-out option, classification of message types and codes, and series details for promotional and transactional calls, among other aspects.

Algorithmic Trading Framework

SEBI issued a Circular dated 4 February 2025, establishing a framework for algorithmic trading by retail investors. The Circular, *inter alia*, includes requirements for the registration of specified trading algorithms, the empanelment of algo providers, and a framework for fee-sharing arrangements between brokers and algo providers. In addition, the framework introduces stringent controls on API access. Open APIs are prohibited. Brokers must allocate unique client and vendor-specific API keys, restrict access to whitelisted static IP addresses, and implement two-factor authentication using open authentication protocols. Finally, for algorithms whose logic is not disclosed to the investor ('black box' algorithms), the algo provider must be registered as a research analyst with SEBI. Any material modification to the algorithm will necessitate fresh registration with the concerned stock exchange.

DigiLocker as a digital public infrastructure for reducing unclaimed financial assets

SEBI issued a Circular dated 19 March 2025, on harnessing DigiLocker as a digital public infrastructure for reducing unclaimed financial assets. The key aspects of the circular involve ability to store and fetch statement of holdings by DigiLocker users, facility for nomination and read-only access to legal heirs, automated notification to nominees and directions to AMCs, RTAs, Depositories and KYC Registration Agencies.

Across the Globe

- India, along with China and other countries signed a '**Joint Statement on Inclusive and Sustainable Artificial Intelligence for People and the Planet**' culminated at the AI Summit 2025 which emphasizes a human-centric, rights-based and ethical approach to development and use of AI systems.

- The European Data Protection Board ('**EDPB**') issued a Statement dated 11 February 2025, in relation to principles to design GDPR-compliant age assurance mechanisms, including tokenized mechanisms that uphold data minimization principles, while effectively implementing age assurance mechanisms.

- Certain parts of the European Union's Regulation 2024/1689, known as the '**AI Act**', has come into force on 2 February 2025. The aspects which are enforced pertain to mandatory AI literacy, prohibited AI practices and prohibition on creation or expansion of facial recognition databases. The rest of the majority provisions of the AI Act are expected to come into force by August 2026.

- The UK Government has launched a consultation to expand an exemption for text and data mining (TDM) that allows AI models to train on publicly available data even for commercial purposes, beyond the 'non-commercial use' qualification under existing copyright law. Rights-holders have been proposed to have opt-out rights in this regard.

Contact Us

Any query relating to the subject of this Update may be directed to:

Noorul Hassan, Partner, Corporate and M&A
E-mail: noorul.hassan@lakshmisri.com

Sameer Avasarala, Principal Associate, Technology & Data Privacy
E-mail: sameer.avasarala@lakshmisri.com

You can also contact us at:

Lakshmikumaran & Sridharan Attorneys
7th Floor, Tower E, World Trade Centre, Nauroji Nagar,
New Delhi 110029, Phone: 011-4129 9800
E-MAIL: Lsdel@lakshmisri.com

Stay Connected

www.lakshmisri.com | www.gst.lakshmisri.com | www.addb.lakshmisri.com

NEW DELHI • MUMBAI • CHENNAI • BENGALURU • HYDERABAD • AHMEDABAD • PUNE • KOLKATA • CHANDIGARH • GURGAON • PRAYAGRAJ • KOCHI • JAIPUR • NAGPUR