Consent Managers Under the DPDPA: Implications for Global Capability Centres

Introduction

India's Digital Personal Data Protection Act, 2023 ("**DPDPA**"), together with the Digital Personal Data Protection Rules, 2025 ("**DPDP Rules**") (collectively, the "**DPDP Framework**"), introduces a new category of regulated intermediary, the consent manager, that has received considerably less attention in the GCC context than it deserves. With full substantive compliance obligations scheduled to take effect by May 2027, and the consent manager registration window opening in November 2026, GCCs that defer operational decisions will find themselves with limited time to get things in place.

This article examines the role of the consent manager, its application to GCCs operating in India, and, more critically, the question that most directly affects how GCCs structure their data compliance programmes: whether consent managers are required for data principals located outside India, and how the answer to that question complicates personal data management for entities processing both Indian and foreign personal data.

What is a Consent Manager?

Under Section 2(g) of the DPDPA, a consent manager is a person registered with the Data Protection Board of India (the "**Board**") who acts as a single point of contact to enable a data principal to give, manage, review and withdraw consent through an accessible, transparent and interoperable platform. Where so opted for by the data principal, the consent manager is the entity accountable to the data principal and must act in a fiduciary capacity on the data principal's behalf.

There are several criteria that entities need to meet to be considered eligible as consent managers, such as being incorporated in India, maintaining a minimum net worth of INR 2 crore, operate independently of any data fiduciary (including affiliated entities), and function on a data-blind basis i.e. they manage and record consent but cannot access, use or monetise the underlying personal data they are facilitating consent for. They are required to register with the Board, and will be subject to technical, operational and governance conditions prescribed under the DPDP Rules.

The construct of consent managers appears to have been drawn conceptually from India's Account Aggregator ecosystem in financial services. The ambition is a cross-sectoral, interoperable consent infrastructure resulting in a single dashboard through which individuals can manage their consent across multiple data fiduciaries, rather than navigating each platform separately. However, the practicality of implementing this is yet to be tested.

How the DPDP Framework Applies to GCCs

The DPDP Framework applies to the processing of all digital personal data within India (ostensibly, irrespective of where the information originates). It also has extra-territorial reach, applying to processing outside India where that processing is in connection with offering goods or services to data principals within India.

For most GCCs, a significant part of the applicability will likely come from the processing activity and the contractual relationship underlying it. Some substantive compliance obligations, including consent requirements and the consent manager construct, do not appear to apply to an Indian entity processing personal data of foreign data principals pursuant to a contract with persons outside India. This carve-out is commercially significant. Without it, GCCs providing back-office, HR, or technology services to a global parent workforce would, for the same processing activity, face overlapping compliance obligations i.e. DPDPA on one side and GDPR or equivalent regimes on the other.

In practical terms, this means that a GCC processing the personal data of employees based in the United Kingdom, Germany or the Netherlands, under a service agreement with its foreign parent, falls outside the consent compliance obligations of the DPDP Framework for that specific processing activity. Consent managers, accordingly, do not enter the picture for such data and those individuals' consent continues to be governed by their home jurisdiction's data protection regime.

Where the Complexity Lies

The carve-out, however, operates at the level of the individual i.e. the data principal and the contractual basis on which the GCC processes the data, not at the level of the GCC as an entity. This distinction is critical, and it is where most GCCs will encounter practical difficulty.

The position is complicated for GCCs that process foreign personal data under contract with the foreign parent (and therefore fall within the carve-out) while simultaneously processing Indian personal data in their own right, whether as an employer, as a contracting party with Indian vendors, or as a service provider to Indian customers. For the latter processing activities, the DPDP Framework applies in full, including the obligation to be capable of interfacing with consent managers where Indian data principals choose to exercise their consent rights through one.

Most large GCCs do not operate segregated data environments for Indian and non-Indian personal data. HR systems, identity and access management platforms, project management tools, payroll infrastructure and communication platforms typically process personal data of a globally distributed workforce on shared infrastructure. Once the substantive consent provisions of DPDP Act come into force, separating what falls within the DPDP Framework's scope from what is carved out will require an ongoing analysis within the GCC's operations.

Practical Implications for GCC Compliance Architecture

It appears that for processing activities that are within scope, GCCs operating as data fiduciaries must be technically capable of receiving and honouring consent signals from any registered consent manager that an Indian data principal chooses to use as the choice of the consent manager rests with the data principal, not the data fiduciary. That being the case, a GCC may not be able to standardise on a single platform or require its Indian employees and counterparties to use a particular consent manager and may need to build interoperable infrastructure capable of connecting with whichever registered consent manager a given individual selects.

For processing activities falling under the foreign-principal carve-out, the DPDP Framework's consent manager provisions do not apply. Foreign data principals' consent rights continue to be governed by the applicable regime in their home jurisdiction, whether that is the GDPR, the UK GDPR, or another equivalent framework. For GCCs serving European parents, this means that GDPR consent mechanisms and the existing data processing agreements with those parents remain the governing framework for those data subjects, entirely separately from India's domestic consent architecture.

The near-term priority for GCCs is identifying, at the activity level, which processing operations involve Indian data principals and are therefore subject to the DPDP Framework. This exercise, combined with a review of the contractual basis for foreign-principal data processing, is necessary for GCCs to have a robust consent management compliance programme, capable of mitigating and limiting liability. GCCs that defer this work until closer to the May 2027 deadline will find the implementation timeline compressed, particularly where there is shared infrastructure which may require systemic level changes rather than incremental process adjustments.

Conclusion

The consent manager framework represents a genuinely novel development in India's data protection landscape and, in our view, demands more attention from GCCs than it has so far received. While the foreign-principal carve-out provides meaningful relief for a significant portion of GCC data processing activity in terms of consent management, it also complicates the operations of GCCs. The compliance work lies in determining, with precision, which processing activities fall within scope, building interoperable infrastructure for those that do, and maintaining the contractual and operational separation that allows the carve-out to operate effectively for those that do not, as well as infrastructure capable of interfacing with a wide variety of consent managers.

Compliance systems therefore need to be thought through and structured carefully.

Disclaimer