jsa
advocates & solicitors

JSA Prism

Privacy and Data Protection

Digital Personal Data Protection Act

Edition XIII

January 2025

Navigating compliance under the Digital Personal Data Protection Act, 2023: Key considerations for Global Capability Centres

India stands as a pivotal destination for Global Capability Centres ("**GCCs**"), playing a significant role in supporting multinational corporations across a spectrum of industries such as information technology, finance, healthcare, and telecommunications. The Digital Personal Data Protection Act, 2023 ("**DPDPA**") and the subsequent Draft Digital Personal Data Protection Rules, 2025 ("**Draft Rules**") mark a transformative moment in India's digital regulatory landscape, underscoring India's vision to establish a robust digital economy while ensuring stringent privacy safeguards.

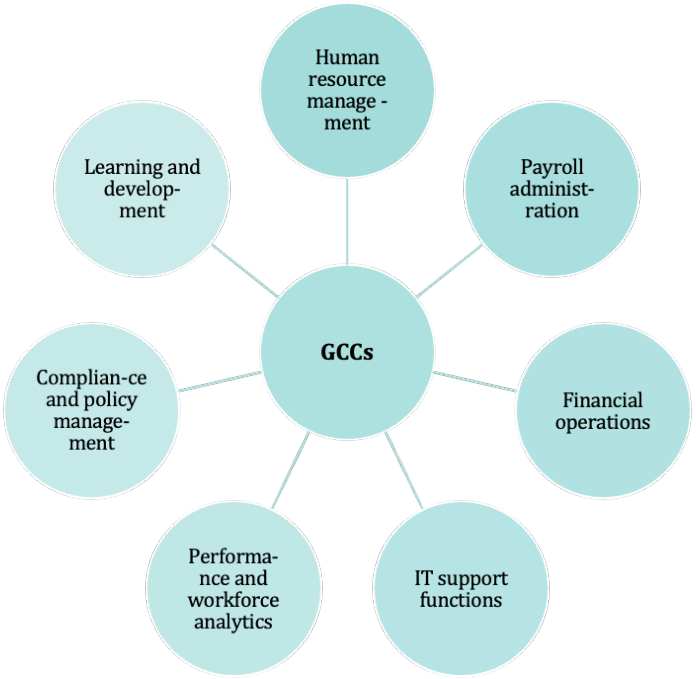
For GCCs, these regulatory developments bring unique challenges and opportunities. GCCs need to comply with the DPDPA while also navigating global laws like the General Data Protection Regulation ("**GDPR**") that may apply to them. In this edition of the Prism, we examine these considerations, explore key compliance requirements, and discuss strategies for aligning with evolving regulatory landscapes.

Key Considerations for GCCs *vis-a-vis* the DPDPA

Handling employee data

GCCs handle extensive volumes of employee data as they serve as centralised hubs for managing critical business functions like human resource, payroll, finance, information technology, training, compliance, and workforce analytics on behalf of multinational organisations. Acting as the operational backbone for such functions, they process data to support global operations, enhance efficiency, and ensure compliance with local and international regulations.

Some of their core employment related operations include:



Under the DPDPA, processing personal data typically requires explicit consent from the data principal. However, the DPDPA recognises certain 'legitimate uses' that exempt organisations from obtaining consent, particularly in the context of employment.

These legitimate purposes include core employment-related activities such as:

- 'the purposes of employment'
- or 'those related to safeguarding the employer from loss or liability such as corporate espionage',
- 'for maintenance of confidentiality of trade secrets, intellectual property, classified information'
- or 'for provision of any service or benefit sought by a data principal who is an employee'

However, if the processing of employee data goes beyond these legitimate uses – for purposes unrelated to core employment functions - explicit consent must be obtained from the employee. It thus becomes important for GCC to document what data is collected, the specific purposes for its use and the legal basis for its processing. This may be essential to demonstrate compliance with the DPDPA and to mitigate the risks associated with any unauthorised or non-compliant data processing.

Cross-border data transfers and data localisation

- Restrictions on cross-border transfer
- Data localisation mandates for significant data fiduciaries
- Exemptions for specific transfers

The DPDPA acknowledges the significance of cross-border data transfers, including for GCCs, while prioritising the protection of personal data. Under the DPDPA, the Central Government is empowered to restrict the transfer of personal data by data fiduciaries to specified countries or territories through notifications. Importantly, the legislation also establishes that its provisions do not override existing sectoral regulations that may impose stricter requirements on data transfers.

The Draft Rules add that the Central Government may prescribe certain requirements even for transfers to approved countries. GCCs must carefully evaluate where employee data is stored and accessed to ensure compliance with these rules.

For GCCs that may be classified as Significant Data Fiduciaries ("**SDFs**") due to the volume or sensitivity of the data they process, the Draft Rules introduces additional obligations. The Draft Rules prescribe that the Central Government may mandate localisation of certain data, along with related traffic data in India. This makes it crucial for GCCs to be more careful if they are classified as SDFs

There are certain exemptions under the DPDPA that may potentially allow GCCs to be exempt from restrictions on cross-border data transfers. For instance, processing personal data may be exempt if it is necessary for enforcing legal rights or claims, or if it involves the processing of personal data related to a contract entered into with a person outside India. These exemptions could be particularly useful for GCCs, where data is frequently transferred across borders for operational purposes. However, GCCs must carefully evaluate each case to ensure they meet the specific conditions of these exemptions and mitigate any potential compliance risks.

Intra-group transfers

GCCs often perform intra-group transfers to centralise and streamline operations, ensuring efficient use of resources and expertise. Such intra-group transfers of data by GCCs must be conducted in compliance with the provisions laid out for data processing under the DPDPA.

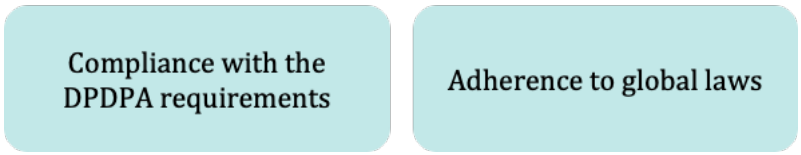
When it comes to group transfers of data, key issues that may arise include maintaining clarity on the legal basis for processing, considering purposes for which personal data may be shared within the group and ensuring that data is transferred outside India in compliance with the DPDPA.

If GCCs already have group policies that align with global laws like the GDPR, these may need to be adapted to meet the DPDPA's requirements, especially where the DPDPA affords more protection or adds restrictions for personal data. To ensure compliance, GCCs may need to review and enhance their internal group transfer policies.

Intersection of global laws and the DPDPA

The intersection of global privacy laws and the DPDPA presents a complex challenge for GCCs, which act as hubs for multinational organisations. As these centres of operations often handle data across various jurisdictions, GCCs are not only required to comply with the data protection regulations of the country they operate in, but also with international laws like the GDPR, United States' Health Insurance Portability and Accountability Act of 1996, California Consumer Privacy Act etc. For example, when processing data of employees in the EU, the GDPR will apply in addition to the DPDPA. Navigating this intersection may require a strategic approach to harmonise policies across diverse legal frameworks while maintaining consistency and compliance. GCCs must carefully consider how global regulations intersect with the DPDPA, particularly in areas such as consent frameworks, data subject rights, data localisation requirements, accountability and cross-border data transfer mechanisms.

Creating globally aligned data policies that incorporate the DPDPA's incremental obligations requires a dual approach:



GCCs may need to develop scalable data governance frameworks that include robust mechanisms for tracking legislative changes in India and abroad. Furthermore, these policies may need to incorporate dynamic compliance monitoring tools and employee training programs tailored to the DPDPA's evolving regulatory landscape.

Third-party/vendor management

GCCs often provide shared services across their global operations, which may involve transferring data received from different countries to downstream vendors, both within India and abroad. As a result, it becomes crucial for GCCs to conduct thorough due diligence on their vendors, ensuring they not only comply with the DPDPA but also adhere to the requirements of relevant global privacy laws. This may include a unified due diligence approach, signing contracts with global protections, an integrated breach management policy and an audit strategy that's globally aligned.

By ensuring that vendor relationships meet both DPDPA and global standards, GCCs can mitigate potential regulatory risks and maintain the integrity of their operations across borders.

The path forward for GCCs

GCCs operate in a complex environment shaped by diverse regulatory requirements and evolving data protection laws. From managing employee data and ensuring lawful cross-border transfers to maintaining oversight over third-party vendors, the challenges are multifaceted and demand careful attention. The DPDPA, Draft Rules, and global laws like GDPR add layers of accountability, requiring GCCs to align their practices with stringent global compliance standards.

Navigating these intricate requirements is not just a regulatory necessity but a critical aspect of sustaining seamless operations. As GCCs continue to expand their roles, addressing these considerations will remain pivotal.

Infotech Practice (Privacy and Data Protection)

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:

Akshaya Suresh
Partner

Drishya A. Kamath
Associate

18 Practices and
41 Ranked Lawyers

7 Ranked Practices,
16 Ranked Lawyers

Elite – Band 1 -
Corporate/ M&A Practice

---

3 Band 1 Practices

---

4 Band 1 Lawyers,1 Eminent Practitioner

12 Practices and
50 Ranked Lawyers

14 Practices and
38 Ranked Lawyers

20 Practices and
22 Ranked Lawyers

Ranked Among Top 5 Law Firms in India for ESG Practice

Recognised in World's 100 best competition practices of 2025

Among Top 7 Best Overall Law Firms in India and
11 Ranked Practices

---

11 winning Deals in
IBLJ Deals of the Year

---

11 A List Lawyers in
IBLJ A-List - 2024

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 #1
The Vahura Best Law Firms to Work Report, 2022

Top 10 Best Law Firms for Women in 2022

7 Practices and
3 Ranked Lawyers

For more details, please contact km@jsalaw.com

jsa
advocates & solicitors

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