Transcending Boundaries: Crafting India's Cross-Jurisdictional Data Protection Strategy

BY: SRIPAL JAIN

CENTRE FOR COMPETITION LAW AND ECONOMICS
AUGUST 2023

Transcending Boundaries: Crafting India's Cross-Jurisdictional Data Protection Strategy

Sripal Jain

Introduction

In an era marked by the rapid growth of digital technologies and the increasing significance of personal data, nations around the world are recognizing the need for robust data protection laws. Recent years have seen groundbreaking regulations such as the European Union's General Data Protection Regulation (GDPR), the draft United States' American Data Privacy Protection Act (ADPPA), and the United Kingdom's Data Protection Regulation (UK DPR). Joining this international trend, India has recently enacted the Digital Personal Data Protection Act (DPDPA) These regulations collectively form a tapestry of legal frameworks that govern the collection, processing, and sharing of personal data, balancing individual privacy rights with societal needs and economic interests. This examination will explore the similarities and differences between these major regulations, with a specific focus on the newly implemented DPDPA in India.

Categorization of Personal Data

The recently released version of the DPDPA 2023 does not make any categorization of Personal Data which was made in its 2018 and 2019 versions. It mandates equal compliance requirements across all types of personal data, emphasizing the implementation of reasonable security safeguards for data protection. This approach reflects a more generalized perspective, where all personal data, regardless of sensitivity, is subjected to the same protection level. It can simplify compliance but might overlook nuanced differences in the nature of various data types. Generally, Special/Sensitive categories of personal data include racial or ethnic origin, political opinions,

religious or philosophical beliefs, trade union membership, health, genetic or biometric data processed for the purpose of identification, sex life, and sexual orientation.

There is synergy regarding categorization in GDPR, ADPPA and UK DPR. GDPR and UK DPR categorized data into Personal Data and Sensitive Personal Data while ADPPA categorized it into ‘Covered Data’ and 'Sensitive Covered Data'. This approach creates a more tailored framework to protect data, focusing specifically on those categories that might require stricter control and consent mechanisms. This can provide more nuanced protection but may complicate compliance efforts.

Age of Children for Parental Consent

The varying regulations for children's personal data protection demonstrate the diverse legal perspectives across jurisdictions. Under the DPDPA, parental consent is mandated for those up to 18 years old, reflecting a cautious approach. In contrast, the GDPR prescribes parental consent for children under 16, allowing member states the choice to lower this to 13 years, thereby offering flexibility within its framework. The UK DPR sets this age at 13 years, aligning with a more permissive view. The ADPPA introduces another dimension by deeming covered data of minors (those under 17) as sensitive, but only when the entity knows the individual's age, focusing more on the nature of the data rather than a strict age limitation. These varying approaches highlight the complexity and context-specific nature of determining appropriate age thresholds for parental consent in data protection.

Classification of Data Fiduciaries

The DPDPA 2023 classifies data fiduciaries into “significant data fiduciaries and “data fiduciaries” based on certain criteria including the volume and sensitivity of personal data processed, risk to the rights of data principal, potential impact on the sovereignty and integrity of India, risk to electoral democracy, security of the State and public order. It prescribes certain additional obligations for significant data fiduciaries including the appointment of a resident data protection officer for grievance redressal, independent data auditor and conducting data impact assessment

(DIAs). GDPR and DPR 2018 do not make any such classification in data fiduciaries, adopting a more uniform and simplified approach.

ADPPA classifies ‘Certain Covered Entities’ as 'large data holders' (LDHs) and covered high-impact social media companies based on certain criteria. It includes companies that make more than $250 million in gross annual revenue, process more than 5 million individuals’ data and process more than 200,000 individuals’ sensitive data. Like DPDPA, it imposes additional requirements on LDHs. Unlike DPDPA, ADPPA also defines Small and Medium Businesses (SMBs), exempting them from these additional obligations.

DPDPA's detailed classification, focusing on potential risks and national concerns, underscores India's emphasis on localized control, individual rights protection, and national security whereas the inclusion of specific criteria for SMBs acknowledges the need to balance privacy protection with business viability, reflecting a more pragmatic and market-oriented approach.

Right to Data Portability

The DPDPA of India with other prominent regulations has excluded the right to data portability in its latest form, a provision that was earlier included in its 2019 draft. Meanwhile, the GDPR, the ADPPA, and the UK DPR all provide for the right to data portability.

The removal of the right to data portability in India's DPDPA may signify a shift in focus towards balancing privacy rights with industry needs, as the provision could present technical and regulatory challenges for service providers. The inclusion of this right in the GDPR, ADPPA, and UK DPR emphasizes the importance of user control and flexibility, allowing individuals to transfer their data between different service providers. The variance in approach between these regulations highlights divergent priorities and strategies related to individual empowerment, technological readiness, and regulatory frameworks.

Penalties

The DPDPA prescribes capped financial penalties of up to INR 250 crores (INR 2.5 billion), without linking to worldwide turnovers and without any provision of compensation to the affected data principal. The GDPR sets penalties up to €20 million or 4% of global annual turnover, while the UK DPA allows fines up to £17.5 million or 4% of annual global turnover, whichever is higher in both cases. ADPPA in the U.S. does not specify fixed penalties but instead treats non-compliance as unfair or deceptive acts under the Federal Trade Commission Act, subject to civil or criminal repercussions.

India's DPDPA, with its fixed cap, may indicate a desire to provide clear limits without tying penalties to the size of the organization, potentially reducing the financial deterrent for large enterprises. GDPR's and UK DPA's more stringent penalties are indicative of the EU's strong commitment to data protection, linking penalties directly to global turnover to ensure that fines are meaningful for organizations of all sizes. The flexible approach in ADPPA, relying on existing trade law, reflects a possibly more market-driven and case-specific perspective.

Compensation to the Data Principal

Under the DPDPA, no compensation is provided to affected data principals. Conversely, both the GDPR and the UK DPA allow for compensation to those affected. Under the ADPPA, if a data breach leads to tangible harm such as financial loss or emotional distress, the affected individual may seek compensation through private legal action.

The DPDPA's absence of compensation provisions underscores a concentration on financial penalties rather than providing restitution to affected individuals. In contrast, the GDPR and UK DPR include compensation mechanisms, reflecting an emphasis on individual rights and organizational accountability towards data subjects.

Right to Erasure and Right to Be Forgotten

The DPDPA permits the right to correction, information, access, and erasure of personal data. The right to access information about personal data allows individuals to request a summary of the data being processed and an overview of the data processors/fiduciaries with whom the data has been shared. This right does not extend to instances where data has been shared with another legally authorized data fiduciary for purposes such as prevention, detection, investigation, or prosecution of offences or cyber incidents.

The GDPR and UK DPR recognize the right to be forgotten and rights concerning information, access, and correction of data while ADPPA diverges, not acknowledging the right to be forgotten but instead focusing on opt-out provisions and rights to access, correct, delete, or transfer data.

DPDPA's nuanced approach to the erasure rights might signify a balance between personal autonomy and legal compliance. GDPR and UK DPR emphasize individual control, granting comprehensive rights over personal data. In contrast, ADPPA's lack of a right to be forgotten but the inclusion of opt-out provisions indicates a focus on enabling consumer choice without imposing an absolute erasure obligation on businesses.

Privacy Notice

DPDPA, provides privacy notices only when personal data is being processed based on consent. The notice given to the Data Principal must include the personal data being processed and its purpose, the manner of exercising rights like the right to withdraw consent at any given time, and how to make a complaint to the Board. This approach puts the focus on consent and provides the Data Principal with essential information related to their rights and the processing of their data.

Despite these similarities, there are distinct differences that set global regulations apart. The GDPR mandates a comprehensive approach that underscores transparency and individual rights within the EU, providing an extensive outline of information. The ADPPA, on the other hand, emphasizes a balance between informing individuals and providing flexibility to businesses, requiring additional information on whether personal data is accessible to specific countries like China,

Russia, Iran, or North Korea. Under the UK DPR, the requirements are closely aligned with GDPR but specifically tailored to the UK context, including specific provisions regarding third-party sharing, international transfers, safeguards, usage, and storage duration. These differences reflect varying priorities and approaches to privacy protection within each jurisdiction.

Cross-Border Transfer of Personal Data

The DPDPA, 2023 allows for the free cross-border flow of data unless any territory is specifically restricted, a shift from the earlier whitelisting approach. It also mentions that if any other Indian law provides a higher threshold for protection or restricts the cross-border transfer of data, that law will prevail.

In contrast, GDPR facilitates cross-border data transfer through various legal channels such as adequacy decisions like legally binding and enforceable instruments between public authorities, binding corporate rules, standard contractual clauses and approved code of conduct and certification mechanisms. ADPPA does not explicitly address cross-border data flow, while the UK's Data Protection Regulation allows or restricts transfers based on factors including the adequacy of decisions, transfer safeguards, and binding corporate rules.

DPDPA's shift to a more open, unless blacklisted strategy may be an attempt to foster international business relationships while retaining the right to curb data flow to certain regions for strategic or security reasons. GDPR's comprehensive structure emphasizes both the protection of individual rights and the facilitation of global commerce, using defined legal channels to ensure the security of transferred data, while the UK's DPR provides a balanced approach that considers public interest and safeguarding mechanisms.

Addressing Data Breach

DPDPA mandates the reporting of all data breaches to the regulatory board and affected data principals without any specific threshold or criteria. It potentially reflects an intent to foster accountability and transparency but might also increase administrative burdens on data fiduciaries.

GDPR and UK DPR adopt a risk-based approach to data breach reporting. While there is no set threshold, breaches must be reported to authorities when there's a risk to the rights and freedoms of the data principals. Data subjects must be notified only if there is a high risk. The distinction between risks and high risks allows for a more targeted response, reflecting an intent to balance the need for transparency with avoiding unnecessary alarm.

ADPPA requires companies to make reasonable efforts to secure information and mandates a specific timeframe for informing authorities and affected individuals about breaches. By setting clear standards, the ADPPA encourages proactive data security measures and offers a structured response framework.

Overall, the various regulations demonstrate a global trend towards enhancing accountability and transparency in the event of data breaches. While the DPDPA calls for blanket reporting whereas the GDPR, ADPPA, and UK DPR have adopted more nuanced approaches that balance the interests of data principals, authorities, and businesses.

Applicability of the Legislation

The DPDPA applies to the processing of 'personal data' in India, whether collected digitally or non-digitally and later digitized. It also extends to digital personal data processed outside India if connected to offering goods or services within the country. However, it does not apply to personal data processed for personal or domestic purposes, or to data made publicly available either by the individual to whom it pertains or by others obligated by Indian law to make it public.

The GDPR governs the processing of personal data in the EU, whether automated or part of a filing system and includes provisions for non-EU entities that engage with EU data subjects by means of offering goods and services and monitoring the behaviours. UK DPA has similar applicability. Meanwhile, the United States' ADPPA applies to "covered entities" such as those under the FTC Act, including non-profit organizations but paradoxically excluding large corporations like banks or airlines and government

The DPDPA focuses on data connected to India with specific exemptions, reflecting domestic concerns. GDPR's and UK DPA's extensive reach, even to non-EU entities, highlights the EU's global influence and strong privacy commitment. The ADPPA's unique applicability to certain entities but not others, such as large corporations, shows a balance between consumer protection and industry interests.

Concept of Consent

Under the DPDPA, the consent given by the Data Principal must be free, specific, informed, unconditional, and unambiguous, reflecting a clear agreement to process personal data for a specific purpose. The legislation removes the provision of deemed consent, incorporates 'legitimate uses', and allows data processing for the specified purpose, including instances where the Data Principal has voluntarily provided data, or for state purposes like subsidies, benefits, or permits. The latter includes conditions where the Data Principal has previously consented or the data is maintained and notified by the State, adhering to proper standards and governance laws.

The regulations for consent in the handling of personal data differ across the GDPR, ADPPA, and UK DPR. GDPR requires consent to be freely given, specific, informed, and unambiguous, with clear language and the ability to be withdrawn at any time. Silence or pre-ticked boxes cannot serve as consent. Under ADPPA, the handling of 'sensitive covered data' mandates an 'affirmative express consent' with no exceptions, binding all companies dealing with the personal information of U.S. citizens. The UK DPR necessitates demonstrable consent for processing personal data, and it must be presented distinctly from other matters in a clear form. Consent can be withdrawn, and utmost consideration must be given to assess whether consent is freely given, especially if linked to a contract or service that does not necessarily require the processing of personal data.

While all the regulations emphasize the necessity for consent to be clear, informed, and revocable, there are distinct variations. The GDPR's focus on unambiguous consent, including rejecting silence or pre-ticked boxes, highlights the EU's strong emphasis on individual rights. The ADPPA's 'affirmative express consent' provision, applicable to all entities dealing with U.S.

citizens' information, underscores a broad and non-exclusionary approach. The UK DPR aligns closely with the GDPR but adds additional layers of complexity related to contracts and services.

Exemptions

Under the DPDPA, exemptions include interests of sovereignty, state security, foreign relations, public order, research, archiving, or statistical purposes, and the Central Government has discretion over the application of certain provisions to specific Data Fiduciaries or startups. The GDPR grants exemptions for processing related to archiving, research, journalism, artistic expression, contract performance, legal obligations, and certain public safety concerns. In the UK DPR, exemptions are allowed if they significantly inhibit an organization's legitimate need for processing data for specific purposes including scientific, historical, statistical and archiving purposes or if it's in the public interest, including permitting automated profiling under legitimate ground

The DPDPA's exemptions cater to India's specific interests in sovereignty and public order, reflecting a tailored approach to national considerations. The GDPR's and UK DPA's wide range of exemptions demonstrates the EU's attempt to align data protection with varied public and individual interests.

Provisions unique to Digital Personal Data Protection Act, 2023

There are provisions in DPDPA like duties of data principals, voluntary undertaking by the data fiduciary, right to nominate, provision of appointing consent managers and right to call for the information by the government, which are conspicuously absent in other global jurisdictions.

Conclusion

The enactment of the DPDPA in India is a significant milestone in the global movement towards comprehensive data protection. Drawing insights from existing frameworks like the GDPR, ADPPA, and UK DPR, India's approach to data protection reflects a unique blend of international best practices and local considerations. The DPDPA, with its nuanced provisions on consent, exemptions, and governance, illustrates India's commitment to aligning with global standards while addressing specific national interests. The varying regulations across these jurisdictions underscore the complex challenge of standardizing data protection in a world marked by diverse cultural, legal, and political landscapes. As the digital era continues to evolve, the ongoing examination and adaptation of these laws will be essential in ensuring that individual privacy is safeguarded, while still fostering innovation, economic growth, and societal well-being.

The writer is Research Intern at Centre for Competition Law and Economics, New Delhi

---

The Centre for Competition Law and Economics

Spacetime, 5th Floor, Savitri Complex
Greater Kailash-II, Delhi-48
centrecomplaw@gmail.com