BLIND FOLD LEGAL JOURNAL

VOLUME 2 ISSUE 3
[MAR 2023 – MAY 2023]

E-mail: blindfoldjournal@gmail.com
Website: www.blindfoldjournal.com

"Examination of India's Data Protection Law: A Partial Analysis of the DPDP Act, 2023 for Businesses"

-Author: Shaswat Verma & Tripti Singh

INTRODUCTION

On August 11, 2023, India introduced the Digital Personal Data Protection Act, 2023 (DPDP Act), heralding a new era in digital personal data processing norms. The DPDP Act is primarily geared towards providing legal recognition to specific facets of informational privacy while ensuring the lawful processing of personal data.

With 44 provisions and a detailed penalty schedule, the DPDP Act will be rolled out in stages, with separate notifications in the Official Gazette. Upon implementation, Section 43A of the Information Technology Act and its corresponding rules, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011 (SPDI Rules), will be repealed. Other relevant data processing regulations, including sector-specific ones, will continue to apply, as long as they do not conflict with the DPDP Act. Additionally, the DPDP Act establishes an independent regulator - the Data Protection Board of India (DPBI) - responsible for its enforcement, investigation, and adjudication. Specific details of the DPDP Act will be addressed through subsequent rule-making.

In this first of two posts, we examine key features under the DPDP Act that businesses need to focus on as they prepare to interpret and comply with this new law.

WHO AND WHAT IS COVERED UNDER DPDP ACT?

The DPDP Act's scope is straightforward. Subject to exemptions, it applies to Data Fiduciaries and Data Processors involved in processing digital personal data within or outside India in specific situations. Here are some key concepts and insights:

Digital Personal Data (PD) encompasses structured representations of information, facts, opinions, or instructions in digital form, pertaining to an identifiable natural person (Data

Principal). This includes data initially collected in non-digital formats that have been subsequently digitized. Pseudonymized data, when combined with identifiers leading to Data Principal identification, is also considered PD under the DPDP Act. Not covered are PD maintained in physical filing systems, anonymized data, and non-personal data.

Sensitive Data Classification: Unlike the SPDI Rules, the DPDP Act does not hinge on whether data is sensitive (e.g., health, financial, biometric). This classification may, however, be relevant in determining Data Fiduciaries and imposing penalties. As a result, organizations not handling sensitive data under existing rules will need to ensure compliance with the DPDP Act.

Processing: This encompasses fully or partially automated operations performed on PD throughout its lifecycle, from collection to destruction. This includes semi-automated processes, whereas non-automated operations are excluded.

Territorial Nexus: If any entity, regardless of its presence or incorporation in India, processes PD within India, it must comply with the DPDP Act. For instance, if a French company processes data of Data Principals in India, the DPDP Act applies.

Exemptions: The DPDP Act does not apply to PD processing for personal or domestic purposes. Additionally, if PD is voluntarily made public by the Data Principal (e.g., social media opinions) or disclosed under applicable law, the Act doesn't apply. The Central Government can also exempt state instrumentalities from the Act for protective reasons like sovereignty or public order. Furthermore, the CG can grant exemptions to specific types of Data Fiduciaries for five years from the commencement date.

CONSENT AS THE PRIMARY BASIS OF PROCESSING

Consent is the primary legal foundation for PD processing according to the DPDP Act. The Act outlines qualitative and technical attributes of valid consent:

Qualitative Aspects: Consent must be free, specific, informed, unconditional, and unambiguous.

Technical Aspect: It must be a clear affirmative action by the Data Principal indicating agreement to PD processing for a specified purpose.

The DPDP Act does not expound on these terms, leading to important considerations for businesses:

Free Consent: It is likely to follow the understanding of "free consent" in the Indian Contract Act, i.e., without coercion, undue influence, fraud, misrepresentation, or mistake. Establishing that consent is indeed free is crucial, with the burden of proof resting on the Data Fiduciary.

Specific Consent: This introduces the principles of purpose limitation and data minimization. Consent should be for identified lawful purposes with a clear scope. It should only pertain to the processing of PD necessary for that specific purpose.

Informed Consent: Transparency is essential. Data Fiduciaries are obligated to provide a notice to Data Principals before or at the time of seeking consent, informing them about various aspects, including the purpose of processing and avenues for withdrawing consent.

Unconditional Consent: Consent should not be made contingent upon the supply of goods or services. Data Principals should have the ability to withdraw consent, and mechanisms for easy withdrawal must be in place.

Unambiguous Consent: The language of consent should be clear and in plain terms. Clear affirmative action is required, indicating deliberate and specific agreement to processing.

DATA PROCESSORS AND THEIR RESPONSIBILITIES

While the DPDP Act places several obligations on Data Fiduciaries, it doesn't specify separate obligations for Data Processors. Instead, it states that Data Fiduciaries can engage Data Processors through valid contracts. Data Fiduciaries remain accountable for the actions and omissions of Data Processors, aligning with global regulatory trends.

To ensure compliance, Data Fiduciaries should conduct detailed data and infosec due diligence before onboarding Data Processors. Detailed data processing agreements, along with periodic audits of the processor's ecosystem, are no longer optional.

CONCLUSION

The DPDP Act's provisions, while awaiting detailed rules, necessitate immediate attention from businesses. Understanding the essence of the Act, reviewing existing processes, and preparing for compliance are critical steps. Many businesses, particularly those not processing sensitive personal data, will face new legal requirements, requiring time for adaptation. Given the absence of a specified transition period, organizations should begin preparations promptly. In our second post, we will delve into Data Fiduciaries' obligations, Data Principals' rights, cross-border transfers, and penalties.