India's new DPDP regime - What GDPR-compliant businesses should know

A. INTRODUCTION

The Digital Personal Data Protection Act, 2023 (**DPDP Act**) along with the Digital Data Protection Rules, 2025 (**DPDP Rules**), notified in November 2025, provides a framework for protection of digital personal data in India. As readers would recall, the DPDP Act and DPDP Rules will be enforced in a phased manner with substantive provisions coming into effect fully by May 2027.

The General Data Protection Regulation (**GDPR**) is the key data protection framework in the European Union (**EU**) and the Indian DPDP framework has broad thematic and principle-based similarities with the GDPR. However, there are notable distinctions between both, and therefore, organizations that claim to be compliant with the GDPR requirements must take into account the differences between both frameworks, particularly those requirements under the DPDP framework which are over and above the GDPR requirements (*i.e.*, GDPR *plus* requirements).

In this primer, we crystallize four noteworthy aspects on which the DPDP is a '*plus*' over the GDPR and the implications for businesses as they prepare towards compliance with the DPDP framework. Needless to say, the primer does not set out *all* the differences between both the frameworks.

B. DPDP 'PLUS' - MORE THAN THE GDPR?

- **Consent for processing - take 'notice'**. Under both frameworks, a request for consent[1] to process personal data[2] must be presented in clear and plain language. There are, however, material differences in the requirements for the contents of a notice between GDPR and DPDP frameworks - while GDPR requires disclosure of a broader set of information, the DPDP requirements for a notice, with a narrower set of information, appear to be more granular. To comply with the DPDP framework, a notice must, therefore, incorporate the specific requirements set out under the DPDP Act and DPDP Rules[3]. The DPDP framework also requires a notice to be made available in English, Hindi, and certain other Indian languages.[4]

[1] Section 6(1) of DPDP Act; Articles 7(1), 7(2) of GDPR.

[2] In the context of the DPDP Act, processing of 'personal data' would mean the processing of 'digital personal data'.

[3] The notice must include (i) an itemized description of personal data; (ii) the specified purpose(s) of processing; (iii) specific description of goods/ services to be provided by such processing; (iv) manner of exercising the right of withdrawal; (v) manner of availing of grievance redressal; (vi) manner in which a complaint can be made to the Digital Protection Board of India (**DPBI**); (vii) details of a 'data protection officer' or any other person authorized to respond to the data principal's communications

[4] The languages listed under the Eighth Schedule to the Indian Constitution, *i.e.*, Assamese, Bengali, Bodo, Dogri, Gujarati, Hindi, Kannada, Kashmiri, Konkani, Maithili, Malayalam, Manipuri, Marathi, Nepali, Odia, Punjabi, Sanskrit, Santali, Sindhi, Tamil, Telugu, and Urdu.

WHAT DOES THIS MEAN FOR BUSINESSES?

Simply put, even if a business complies with the GDPR's notice requirements, it must still deploy a notice that meets the requirements of the DPDP Act and DPDP Rules for any processing that falls within the DPDP framework.

- **Processing - On what grounds?** There is significant overlap between the GDPR and DPDP frameworks as regards the grounds for processing of personal data. Under both frameworks, processing can be undertaken based on 'consent' or on certain other grounds for which consent is not required. The GDPR recognizes two notable grounds for processing that are absent under the DPDP:
  - ***Processing personal data for contractual necessity.*** The GDPR permits the processing of personal data without consent, where such processing is necessary for performance of a contract with the data subject.[5][6] The DPDP Act, however, does not recognize 'contractual necessity' as a specific ground for processing without consent.[7] In the Indian context, this exclusion seems to reflect the concern that standard form contracts may unilaterally incorporate clauses on unrelated processing even if such processing is not necessary for performing the contract[8] (*for a more in depth view on this ground of processing in the DPDP context, please see our previous primer*).
  - ***Processing personal data for a controller's legitimate interest.*** The GDPR also allows processing of personal data of a data subject without consent if necessary for a controller's legitimate interest, unless such a legitimate interest is overridden by the data subject's interest or fundamental right.[9] Notably, this ground has been excluded under the DPDP framework considering its subjectivity and difficulty in enforcement.[10]

WHAT DOES THIS MEAN FOR BUSINESSES?

When processing personal data under the DPDP Act, businesses should identify the legal basis for such processing:

- *Is the processing based on valid consent of a data principal?*
- *If not, does it fall within one or more of the "legitimate uses" identified under the DPDP Act?*

If neither of the above applies, the processing may not comply with the DPDP framework. Business should note that certain grounds for processing recognised under the GDPR (e.g., contractual necessity or legitimate interest) do not qualify as a valid basis under the DPDP Act. Accordingly, processing activities should be independently assessed for compliance under the DPDP framework.

- ***Children's personal data - watch where you step?*** Both the GDPR and DPDP frameworks mandate obtaining 'verifiable' consent from the parent (or lawful guardian) in case of processing children's personal data.[11] Under the GDPR, children are individuals below 16 years of age, however, under the DPDP Act, children are individuals below 18 years of age. Under the GDPR, parental consent is required if a child's personal data is processed in relation to 'information society services'[12] which include a wide array of services, with certain exclusions[13]. Unlike the GDPR, under the DPDP framework, processing a child's personal data, for any purpose, would require verifiable consent (subject to certain prescribed exemptions).

---

5 'Data subject' under the GDPR is the same as 'data principal' under the DPDP Act.
6 Article 6(1)(b) of GDPR.
7 Section 7 of DPDP Act.
8 Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, Chapter 3, B.II.(g), pgs. 40-42, available here.
9 Article 6(1)(f) of GDPR.
10 White Paper of the Committee of Experts and a Data Protection Framework for India, Chapter 4.4, pgs. 103-104, available here.
11 Section 9 of DPDP Act; Article 8 of GDPR.
12 'Information Society Services' as defined under Article 1(1)(b) of the Directive (EU) 2015/1535 of the European Parliament and of the Council as service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services, with certain exclusions (as provided under this Directive).
13 These services include medical examinations, electronic games in a video arcade, automatic cash or ticket dispensing machines, voice telephony services, television/ radio broadcasting services etc.

WHAT DOES THIS MEAN FOR BUSINESSES?

Given the higher age threshold under the DPDP framework, GDPR compliance alone will not suffice. To ensure compliance with the DPDP framework, businesses must ensure that verifiable consent is obtained for processing children's (i.e., individuals below 18 years) personal data for any purpose, unless an exemption applies.

- ***Data breach.*** In the event of a breach of personal data,[14] a data fiduciary must notify the DPBI and every affected data principal, with the required details and without delay.[15] After the initial notification, the data fiduciary is required to submit a detailed intimation to the DPBI within 72 hours (or a longer period if so permitted) of becoming aware of the breach. In contrast, the GDPR has a risk-based approach, requiring a notification to the supervisory authority only if there is a "risk" to natural persons, and notification to data subjects only if there is a "high risk" to rights and freedoms.[16] The GDPR provides carve-outs to notify data subjects if envisaged measures have been taken and even permits a public communication of the data breach if individual notifications would involve a disproportionate effort.[17]

WHAT DOES THIS MEAN FOR BUSINESSES?

On data breach reporting, the DPDP framework sets a higher bar than the GDPR, mandating reporting without any consideration of risk thresholds, unless an exemption applies. As a result, robust organizational protocols for data breach responses and incident management are essential to ensure compliance.

C. CONCLUSION

The DPDP framework signals a momentous shift in India's data protection landscape. Businesses processing personal data in India or processing personal data outside to offer goods/ services in India would have to comply with its requirements. The DPDP framework has a unique compliance architecture and an existing GDPR compliant business model will not automatically translate into DPDP compliance. Understanding the DPDP framework's distinct requirements will be critical to not only manage legal risks but also embed robust data governance practices.

We hope you have found this information useful. For any queries/clarifications please write to us at insights@elp-in.com or write to our authors:

Ravisekhar Nair, Partner – Email -ravisekharnair@elp-in.com

Parthsarathi Jha, Partner – Email - parthjha@elp-in.com

Aayushi Sharma, Principal Associate- Email – aayushisharma@elp-in.com

Priyanjali Singh, Associate- Email- priyanjalisingh@elp-in.com

[14] Section 2(u) of DPDP Act defines 'personal data breach' to state any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.
[15] Section 8(6) of DPDP Act and Rules 7 of DPDP Rules.
[16] Article 33, 34 of GDPR.
[17] Article 34(3)(c) of GDPR.