May 2024

DUA ASSOCIATES

IN BRIEF –
CROSS-BORDER DATA TRANSFER REGIME UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Brief Introduction to the Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDPA), aims to provide safeguards in the processing of digital personal data, in a manner that recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto. One of the key considerations of the DPDPA is its impact on cross-border data transfers. The data protection mechanism as set out under the Information Technology Act, 2000 (IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 prescribe compliances for transfer of personal data which is categorized as sensitive personal data or information. The DPDPA cross-border transfer restrictions, however apply to all kinds of personal data (*including personal data that may not ordinarily be classified as critical or sensitive*).

On August 7, 2023, the DPDPA was passed by the Lok Sabha and subsequently on August 9, 2023 by the Rajya Sabha. On August 11, 2023, the President of India, granted assent to the DPDPA. At present, the Act is yet to come into force and the rules that will further clarify the implementation aspects of cross-border data transfers are still awaited. Once the aforesaid come into effect (dates yet to be notified), the DPDPA read with its rules will replace the current data protection mechanism as provided under the IT Act and the rules.

I. <u>Cross-Border Data Protection under the DPDPA</u>

A law on cross-border data protection involves ensuring the safe movement of personal and electronic data around the world. In many countries, legislatures have attempted to regulate cross-border data transfers by imposing restrictions on transfers of personal data to other countries that do not have similar data privacy laws. Many a time, data localization requirements have been put in place so that data or copies of data remain in the country of origin.

Section 16 (under Chapter IV – Special Provisions) of the DPDPA envisage processing of personal data outside India. Section 16 reads as follows:

"16. (1) The Central Government may, by notification, restrict the transfer of personal data by a 'Data Fiduciary' for processing to such country or territory outside India as may be so notified.

(2) Nothing contained in this section shall restrict the applicability of any law for the time being in force in India that provides for a higher degree of protection for or restriction on transfer of personal data by a 'Data Fiduciary' outside India in relation to any personal data or 'Data Fiduciary' or class thereof."

Section 16(1) of the DPDPA cites territorial restrictions. This could possibly relate to restrictions in the form of prescribing additional compliances for the transfer of personal data to the notified countries or limiting the transfer of certain types of data, but in its present form, the DPDPA is silent on what restrictions it would impose.

Under the said provision, while cross-border transfers of personal data are permitted, it is pertinent to note that the said Section 16 enables the Government to restrict the transfer of personal data to certain countries or territories outside India by way of a notification in the Official Gazette. In other words, transfer would be permissible to all countries until any of them is prohibited by the Government by way of a notification.

The DPDPA is designed to have extra-territorial applicability, which extends to foreign companies outside India. Considering that basic personal data would be required for providing goods and/ or services, foreign companies which are present in those countries to which personal data is not permitted to be transferred, when notified by the Government, may find it difficult to undertake business in relation to India. If data is already being transferred to a country that

the Government subsequently restricts the transfer to, there would be an urgent action that should be taken to stop the said transfer.

Compared with earlier iterations of the DPDPA at the stage of it being a bill, which insisted on localization requirements for certain categories of critical personal data, the DPDPA substantially has relaxed the data transfer obligations.

When Section 16(2) of the DPDPA is carefully examined, it elucidates that that if any other prevailing Indian law(s) stipulate/s for a higher degree of regulation or compliance with respect to the transfer of personal data outside India, then such requirement will take precedence over the DPDPA. The intention is to avoid any probable disputes with laws already enforced. In other words, Section 16(2) of the DPDPA focuses on prevailing laws which have stricter data protection measures when transferring data abroad. To cite an example, the Reserve Bank of India issued a directive by way of Circular DPSS.CO.OD.No 2785/06.08.005/2017-18 dated April 6, 2018, on the 'Storage of Payment System Data', advising all system providers to ensure that, within a period of 6 (six) months, the entire data relating to payment systems operated by them is stored in a system only in India (RBI Directive). The RBI Directive will take precedence over the DPDPA in relation to storage of Payment System Data.

Similar to the RBI Directive, certain categories of telecommunication data, including accounting information related to subscribers, cannot be transferred outside India. In the insurance sector as well, there are equivalent localization requirements (under the Insurance Regulatory Development Authority (Maintenance of Insurance Records) Regulations, 2015). Despite the lack of data localization obligations set out under the DPDPA, all such restraints will continue to apply.

II. Exemptions under the DPDPA from Cross-Border Data Transfer Restrictions

Section 17 of the DPDPA provides exemptions from cross-border data transfer restrictions under following circumstances:

- Legal right or claim enforcement: The processing of personal data is deemed necessary for enforcing any legal right or claim;
- Processing pursuant to contract: Personal data of data principals not within the territory of India may be processed pursuant to any contract entered into with any person outside the territory of India, by any person based in India;
- Court approved corporate restructuring: The processing of personal data may be necessary for a scheme of compromise or arrangement or merger or amalgamation of two or more companies or a reconstruction by way of demerger or otherwise of a company, or transfer of undertaking of one or more company to another company, or involving division of one or more companies, approved by a court or tribunal or other authority competent to do so by any law for the time being in force;
- Judicial/ Quasi-judicial / Regulatory function: The processing of personal data by any court or tribunal or any other body in India which is entrusted by law with the performance of any judicial or quasi-judicial or regulatory or supervisory function, where such processing is necessary for the performance of such function, is permitted;
- Debt recovery: The processing of personal data for the purpose of ascertaining the financial information and assets and liabilities of any person who has defaulted in payment due on account of a loan or advance taken from a financial institution, subject to such processing being in accordance with the provisions regarding disclosure of information or data in any other law for the time being in force, is also permitted; and
- Prevention/ Detection/ Investigation of offence: Personal data may be processed in the interests of prevention, detection, investigation or prosecution of any offence or contravention of any law for the time being in force in India.

III. Cross-Border Data Transfer under the EU General Data Protection Regulation (GDPR) vis-à-vis DPDPA

As the GDPR is a European Union regulation on privacy in the European Union (EU) and the European Economic Area (EEA), it governs the transfer of personal data outside the EU and the EEA. Under the GDPR, in order to transfer personal data outside the EU and EEA, the controller must: (a) carry out an appropriate transfer mechanism (e.g., standard contractual clauses adopted by the European Commission or the UK equivalent); (b) implement a transfer impact assessment; and (c) depending on the transfer impact assessment outcome, implement supplementary measures (e.g., encryption of data in transit and at rest).

On the contrary, the DPDPA allows for transfers of personal data to all countries, unless that country is included on the Government's list of countries to which data transfers are restricted. Unlike the GDPR, the DPDPA does not provide for specific transfer mechanisms, which we understand is a key gap of the DPDPA in comparison to the GDPR. It is however expected that additional guidance in the form of rules (under the DPDPA) from the Government will most likely cover this aspect.

IV. Penalties for breaches involving Cross-Border Data Transfer under the DPDPA

As per the Schedule to the DPDPA, a fine of up to INR 50 crores (USD Six million approx.) can be imposed in case of a breach involving cross-border data transfer.

This newsletter has been contributed by:

Iqbal Tahir & Gaurav Kapur, Partners at Dua Associates, Gurugram

For further information contact:

Iqbal Tahir, Partner, Dua Associates, Gurugram
E-mail : Iqbaltahir@duaassociates.com
Stay connected with Dua Associates - www.duaassociates.com