Cross-Border Data Transfers Under the DPDP Act: What Businesses Need to Know?

Modern day businesses operate in a highly global and interconnected world. With the seamless flow of information across borders, businesses are able to operate efficiently across multiple jurisdictions and manage their day-to-day operations including cloud storage, customer support, and analytics.

The Digital Personal Data Protection Act, 2023 (**DPDP Act**), along with the Digital Personal Data Protection Rules, 2025 (**DPDP Rules**), sets out India's new legal architecture for the processing[1] of digital personal data.[2] This framework also regulates the flow of digital personal data outside India. One of the most closely watched components of this framework has been the rules surrounding cross-border data transfers and the extent to which the data localization requirements may be imposed.

CAN DATA FIDUCIARIES[3] TRANSFER PERSONAL DATA OUTSIDE INDIA?

Yes, cross-border digital personal data transfers are permitted under the DPDP Act, but such data cannot be transferred to those countries that the Central Government prohibits by way of a notification.[4] While the DPDP Act effectively adopts a **'blacklist' approach** to cross-border data transfers and imposes certain restrictions, it largely preserves the flexibility of the businesses to ordinarily decide where they wish to process personal data.

This is different from the data transfer norms under the European Union's General Data Protection Regulation (**GDPR**), which permit transfers only to such jurisdictions that have adequate level of data protection.[5]

[1] Section 2(x), DPDP Act defines '***processing***' as wholly or partly automated operation or set of operations performed on digital personal data, including collection, recording, organization, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

[2] Section 2(n), DPDP Act defines '***digital personal data***' as personal data in digital form. Section 2(t) defines '***personal data***' as any data about an individual who is identifiable by or in relation to such data.

[3] Section 2(i), DPDP Act defines a '***data fiduciary***' as a person who alone or in conjunction with any other person determines the purpose and means of processing personal data.

[4] Section 16(1), DPDP Act.

[5] Article 45, GDPR, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Additionally, organizations designated as significant data fiduciaries[6] may be restricted by the government from transferring certain categories of personal data (including the traffic data associated with such processing) outside India.[7]

ARE THERE ANY EXEMPTIONS TO THE CROSS-BORDER DATA TRANSFER PROVISION?

Yes, there are certain exemptions from cross-border restrictions, if the personal data processing is carried out for any of the following purposes:

- It is necessary for enforcing a legal right or claim,
- It is undertaken in the interest of prevention, detection, investigation, or prosecution of offences,
- It is necessary for a court-approved merger, amalgamation, business transfer, or reconstruction,
- It involves the processing of personal data of data principals located outside India by a person in India under a contract entered with a person outside India, or
- It is necessary for ascertaining financial information relating to an individual who has defaulted on a loan, and the processing complies with other applicable laws.

HAS A NOTIFICATION WITH A BLACKLIST BEEN ISSUED BY THE GOVERNMENT?

No, the government has not issued such a list so far. As the provisions of the DPDP Act concerning cross-border data transfer will become effective in May 2027, we can expect the list to be issued in due course.

ARE THERE ANY OTHER NORMS APPLICABLE TO THE CROSS-BORDER TRANSFER OF PERSONAL DATA?

Yes. India's current data protection landscape is governed by a mix of general and sector-specific norms.

- **General norms**. The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (**SPDI Rules**) will remain operational until May 2027, when the DPDP Act replaces them.[8] The SPDI Rules prescribe that **sensitive** personal data[9] may be transferred only to countries that provide a comparable level of data protection.[10]
- **Sector-specific norms**. Several regulators already impose data localization obligations. These will continue to apply even after the DPDP Act is in full force, as it explicitly allows applicability of other laws providing for higher degree of protection / restriction on cross-border data transfer.[11] Therefore, for a data fiduciary operating in regulated sectors, compliance will depend on a combined reading of the DPDP Act and the relevant sectoral regulations.

[6] Section 2(z) read with Section 10 of the DPDP Act defines a '***significant data fiduciary***' as such a data fiduciary that the government designates based on criteria such as volume, sensitivity of data being processed. The government has not designated any data fiduciary as significant data fiduciary yet.

[7] Rule 13(4), DPDP Rules.

[8] Section 44(2), DPDP Act.

[9] Rule 3, SPDI Rules defines '***sensitive personal data***' as information relating to password, financial information such as bank account or credit card or debit card or other payment instrument details, physical, physiological and mental health condition; sexual orientation; medical records and history; or biometric information.

[10] Rule 7, SPDI Rules.

[11] Section 16(2), DPDP Act.

For instance, the Reserve Bank of India (**RBI**) mandates that all payments data be stored exclusively on servers located in India,[12] allowing only limited processing overseas.[13] The insurance sector faces similar restrictions, with the Insurance Regulatory and Development Authority of India (**IRDAI**) restricting the offshore storage of policyholder and claims data.[14]

WHAT PREPARATORY STEPS CAN BUSINESSES TAKE IN THE MEANTIME?

Although the DPDP Act is not operational yet and the government has not notified the countries to which personal data cannot be transferred, the businesses should take proactive steps to prepare for multiple scenarios, especially since transferring data across borders and modifying vendor systems can take time. Some recommended steps include:

- **Map cross-border data flows**. Businesses must identify all jurisdictions where the personal data of the data principals[15] is stored or processed. This includes data processed by third parties on their behalf, such as cloud service providers. Comprehensive mapping will expedite the process of transferring the personal data if the government issues a notification restricting certain countries. This step is particularly important for data fiduciaries operating in multiple countries and those that routinely transfer personal data abroad.

- **Put together data localization plans**. If a business is likely to be designated as a significant data fiduciary, it should begin preparing a plan to implement data localization. This includes assessing the feasibility of local storage solutions, hybrid-cloud or multi-region configurations, and evaluating vendor readiness to support Indian data centers.

- **Revisit and update contracts with vendors**. Consider revisiting the existing contracts with third-party service providers, especially those located overseas, to provide for contingency clauses permitting migration of data to India or to other countries that are not restricted by the government, obligations on vendors to support transition within defined timelines, and commitments to comply with DPDP Act. Such provisions will help prevent operational disruptions, if a country where the data is being stored/processed is placed in the list of restricted countries by the government.

- **Build internal awareness among technology and procurement teams.** Cross-border data transfer restrictions impact procurement, outsourcing, cloud infrastructure, and day-to-day business operations. Relevant teams should be sensitized and prepared to conduct preliminary assessments of whether a potential service provider will transfer personal data outside India before onboarding them.

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*

Abhay Joshi, Partner – Email - *AbhayJoshi@elp-in.com*

Bhaavi Agrawal, Senior Associate – Email *- bhaaviagrawal@elp-in.com*

[12] RBI directive on storage of payment system dated April 6, 2018, available at https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244

[13] RBI clarifications on storage of payment system data dated June 26, 2019, available at https://www.rbi.org.in/commonman/English/Scripts/FAQs.aspx?Id=2995

[14] Regulation 3(9), IRDAI (Maintenance of Insurance Records) Regulations, 2015, available at https://irdai.gov.in/document-detail?documentId=604674

[15] Section 2(j), DPDP Act defines '***data principal***' as an individual whose personal data is being processed.