FROM ADEQUACY TO ASSESSMENTS: CROSS-BORDER DATA TRANSFER REGIMES IN INDIA AND EUROPE

Vedika Rathi, Ms. Government Law College, Mumbai

I. INTRODUCTION

In the 21st century, with the proliferation of technology in every sector and the ever-increasing reliance on data-centric operations, safeguarding individuals' privacy and ensuring the security of their personal information has become essential. The demand for seamless data movement, spurred by this connectivity, has erased geographic boundaries. This has spurred worldwide data protection laws amid rising worries from governments and people about personal data security. India's Digital Personal Data Protection Act (**D.P.D.P Act**[1]) and the European Union's General Data Protection Regulation (**G.D.P.R**)[2] are significant data protection frameworks addressing these challenges, each reflecting the social and economic fabric of its country. The foundation of the D.P.D.P Act stems from the landmark *Justice K.S. Puttaswamy (Retd.) v. Union of India*[3] (2017) judgment, in which the Supreme Court of India held informational privacy as a vital facet of the right to privacy.

While the DPDP Act marks a significant step forward, it is not without its challenges, particularly its silence on the criteria for listing restricted countries for data transfers under Section 16. This ambiguity raises a key question: What criteria will the Central Government use to determine which countries are restricted? Adding to these concerns, organisations find DPDP compliance extra tough because it overlaps with rules from other regulators, such as Reserve Bank of India (**RBI**), which requires payment data to stay in India, Insurance Regulatory and Development Authority of India (**IRDAI**) sets its own data rules for insurance, and Securities and Exchange Board of India (**SEBI**) controls data in the stock market—creating a multi-framework compliance challenge that demands meticulous coordination. The

[1]Parliament of India, Ministry of Electronics and Information Technology (MeitY). (2023). Digital Personal Data Protection Act, 2023.
[2]European Parliament, Council of European Union, General Data Protection Regulation.
[3]*Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017, (2017) SCC OnLine SC 996.

provisions in relation to the cross-border data transfer of personal data will be effective from May 13, 2027. This gives ample amount of time to organizations to tailor their privacy policies and compliance strategies in accordance with the provisions of the Act.

II. OVERVIEW OF CROSS-BORDER DATA TRANSFERS UNDER THE D.P.D.P ACT

The D.P.D.P Act allows the overseas transfer by a Data Fiduciary[4] of personal data from India to countries specified by the Central Government, except to jurisdictions which are notified as being restricted, ensuring that the data is protected while maintaining the Indian data protection domestic standards[5]. This section is inspired by Article 45[6] of the G.D.P.R., but gives the Central Government unfettered powers and discretion to assess the adequacy of the overseas recipient's data protection regime. The Digital Personal Data Protection Rules, 2025[7] ("**Draft Rules**") fail to spell out when these notifications will be issued and on what factors will be assessed by the Central Government.

While the provision permits cross-border data transfers to overseas recipients from India, it fails to address the subsequent transfers that may occur once the data reaches the overseas recipient. For instance, consider a scenario where India transfers data to a legitimate recipient, but when the legitimate recipient wants to further transfer the data for legitimate purposes, such "onward transfers" do not yet fall under the ambit of the D.P.D.P Act. In contradistinction to this, the G.D.P.R defines "onward transfers"[8] which will be discussed at a later stage.

The D.P.D.P Act recognizes that nothing in the Act prevents the application of any other Indian law that offers a higher level of protection or imposes stricter restrictions on transferring personal data outside India, concerning any personal data, data fiduciary, or category thereof[9]. Legally, this implies three things. First, the D.P.D.P Act does not impose a blanket uniform data localization requirement for all personal data; second, it does not create a statutory requirement that personal data may be transferred to jurisdictions approved by the Central

[4]Digital Personal Data Protection Act, 2023, s 2(i). "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.
[5]Digital Personal Data Protection Act, 2023, s 16.
[6]General Data Protection Regulation, art. 45.
[7]Parliament of India, MeitY. Digital Personal Data Protection Rules, 2025.
[8]General Data Protection Regulation, art. 44.
[9]Digital Personal Data Protection Act, 2023, s 16(2).

Government; third, companies may nevertheless face stricter data localization restrictions under sector-specific or other Indian laws because the D.P.D.P Act[10] does not override those laws. For instance, IRDAI mandates that all original policyholder records should continue to be maintained in India[11]; IRDAI requires insurers to hold records held in electronic form about policies issued in data centres located and maintained in India[12].

The D.P.D.P Act establishes the Data Protection Board of India ("**D.P.B.I**")[13] as an independent body[14]. While it has various responsibilities, it has not yet been conferred with any authority to review or challenge the Central Government's notification under Section 16. Consequently, there is no forum for data fiduciaries to scrutinize grievances related to politically motivated blocklists and restrictions. Rule 14[15] of the Draft Rules operationalize Section 16 of the D.P.D.P Act by prescribing the conditions under which personal data may be transferred outside India. Rule 14 gives practical effect by requiring data fiduciaries to adhere to Central Government-imposed conditions by a general or a special order before sending data abroad. This Rule reinforces an executive-centric framework by not stating which requirements the data fiduciary needs to adopt.

III. OVERVIEW OF CROSS-BORDER DATA TRANSFERS UNDER THE G.D.P.R

The G.D.P.R was adopted by the European Union (EU) on April 27, 2016, and became applicable on May 25, 2018. The GDPR revolutionized the laws related to data privacy across Europe and beyond. G.D.P.R addresses the needs of a constantly evolving digital landscape, which the 1995 Directive of the EU[16] failed to address. The regulations with respect to cross-border transfers are delineated in Chapter V (Articles 44 – 49) of the G.D.P.R[17]. The regulations allow, without any specific authorisation, the transfer of personal data to overseas recipients whose legal systems have an adequate level of protection. When assessing the adequacy of the level of protection, the European Commission ("**Commission**") takes into

[10]Digital Personal Data Protection Act, 2023, s 16(2).
[11]IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017, regulation 18.
[12]IRDAI (Maintenance of Insurance Records) Regulations, 2015, regulation 3(9).
[13]Digital Personal Data Protection Act, 2023, s 18.
[14]Digital Personal Data Protection Act, 2023, s 28(1).
[15]Digital Personal Data Protection Rules, 2025, rule 14.
[16]European Parliament and Council of European Union, Directive 95/46/EC.
[17]General Data Protection Regulation, Chapter V; Transfers of personal data to third countries or international organisations.

account the following elements: the recipient's legal framework, including its respect for the rule of law, fundamental freedoms, and data protection standards[18], the existence of an independent and effective supervisory authority responsible for enforcing those standards[19], and the recipient's international commitments relating to the protection of personal data[20]. These criteria ensure that adequacy decisions are based on objective and transparent factors.

The Commission, as an implementing Act, may decide that an overseas recipient boasts an adequate level of protection. Such an Act is subject to periodic review at least every four years and must specify its territorial or sectoral scope, including the relevant supervisory authorities where applicable[21]. In the absence of such an implementing Act, the Commission allows transfers where appropriate safeguards and data subject rights are in place[22]. These safeguards may include Binding Corporate Rules (BCR)[23], standard data protection clauses approved by the Commission in accordance with Article 93(2)[24], which states that the Commission will be assisted by a committee to ensure fairness[25], legally binding arrangements between public bodies[26], approved codes of conduct[27], or certification mechanisms accompanied by binding commitments[28]. This framework allows international data flows while ensuring that personal data remains subject to a level of protection comparable to that guaranteed within the EU. The Commission must monitor developments in nations and international organisations that could affect the above-mentioned implementing Acts[29]. The Commission shall, following the periodic review[30] finds that a nation and an international organisation do not have an adequate level of protection, to the extent necessary, repeal, amend, or suspend the implementing Act after consulting the concerned jurisdiction, where appropriate[31].

IV. DPDP ACT AND GDPR: A COMPARATIVE PERSPECTIVE

[18]General Data Protection Regulation, art. 45(2)(a).
[19]General Data Protection Regulation, art. 45(2)(b).
[20]General Data Protection Regulation, art. 45(2)(c).
[21]General Data Protection Regulation, art. 45(3).
[22]General Data Protection Regulation, art. 46(1).
[23]General Data Protection Regulation, art. 46(2)(b) and art. 47.
[24]General Data Protection Regulation, art. 93(2).
[25]General Data Protection Regulation, art. 46(2)(c).
[26]General Data Protection Regulation, art. 46(2)(a).
[27]General Data Protection Regulation, art. 46(2)(e).
[28]General Data Protection Regulation, art. 46(2)(f).
[29]General Data Protection Regulation, art. 45(4).
[30]General Data Protection Regulation, art. 45(3).
[31]General Data Protection Regulation, art. 45(5) and (6).

Currently, India's framework governing cross-border data transfers is in a nascent stage. The contrast with the G.D.P.R is instructive. As India develops its approach, it must balance its unique social and economic needs, including the goals of boosting the digital economy and overcoming infrastructure gaps in data processing without jeopardizing national sovereignty, global integration, economic growth, and the digital ecosystem. The contours of India's cross-border transfer regime remain uncertain pending further notifications from the Central Government. Given the Central Government's objective of enhancing the ease of doing business[32], the upcoming framework may draw upon mechanisms similar to those present in the G.D.P.R or China's assessment-based model[33], or a uniquely Indian approach, a specific consent requirement for cross-border transfers, which may or may not read into existing consent requirements under the Act[34], and some alternative recognition of protection, such as BCRs. BCRs will enable transfers to countries where an adequate data protection framework is not as secure. Until such restrictions are introduced, cross-border transfers remain generally permissible under the Act.

The best way for companies and organizations to go about during this interim duration is to build a consent infrastructure and map their data flows. They should direct their effort into properly complying with existing regulations of the Act, particularly those referring to lawful processing, which involves seeking valid and informed consent[35]. This emphasis on informed consent is especially significant when viewed against the position under the Information Technology Act, 2000, which required specific consent for the transfer of 'sensitive personal data or information'[36].

Organizations should ensure that consent notices clearly disclose any intended transfer of personal data outside India, identify the recipient country or data fiduciary, and specify the purpose of such a transfer which should be consistent with the purposes communicated at the time of collection. Their privacy policy should include the implications of such a transfer and not just a generic statement that the data will be shared with third-party service providers or

[32]Money Control, *Data Draft Bill tries to balance ease of doing business, privacy and national security*.
[33]People's Republic of China, 2021, Personal Information Protection Law.
[34]Digital Personal Data Protection Act, 2023, s 6.
[35]ibid.
[36]Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, rule 7. See also, General Data Protection Regulation, art. 49(1).

with organizations globally. The notice should disclose the period for which the transferred data will be retained and inform Data Principals[37] of the rights available to them in relation to their personal data.

The consent notices already in place for cross-border transfers should be audited. The consent notices for such transfers should also include a clause for withdrawal of consent[38], the overseas recipient should immediately cease the processing of data, and if an erasure[39] has been requested, then delete the data without unreasonable delay. For instance, consider a Software-as-a-Service human resources platform that processes payroll information of employees in India using cloud infrastructure hosted on Amazon Web Services' United States-East region. While such a transfer may be permissible under Section 16 of the Act, the consent notice provided to employees at the time of onboarding must clearly disclose that their personal data will be transferred outside India.

Restrictions should be confined to transfers involving jurisdictions with documented risks to data security where no sufficient commitments are in place. This approach would allow Indian companies to operate globally and prevent unnecessary barriers to the free flow of data while safeguarding individual privacy in high-risk situations.

V. CONCLUSION

This comparison of the D.P.D.P Act and the G.D.P.R offers invaluable insights into how privacy and data protection laws are ever-changing globally. The D.P.D.P Act is unquestionably a significant first milestone in the development of Indian privacy legislation. It codifies and regulates the collection, processing, and management of digital individual data. However, in an age of Artificial Intelligence where data is the new oil, its ultimate effectiveness will depend not only on its statutory framework but also on its implementation, regulatory enforcement, and the manner in which practical roadblocks are addressed in the years ahead.

[37]Digital Personal Data Protection Act, 2023, s 2(j) "Data Principal" means the individual to whom the personal data relates and where such individual is— (i) a child, includes the parents or lawful guardian of such a child;
(ii) a person with disability, includes her lawful guardian, acting on her behalf.
[38]Digital Personal Data Protection Act, 2023, s 6(4).
[39]Digital Personal Data Protection Act, 2023, s 12.