



The Dialogue™

INFORM ENGAGE IDEATE

# PRINCIPLE-BASED FRAMEWORK TOWARDS CROSS-BORDER DATA TRANSFERS

RESEARCH REPORT

AUTHORS : KAMESH SHEKAR | AYUSH TRIPATHI | BHAVYA BIRLA | ESHANI VAIDYA





# PRINCIPLE-BASED FRAMEWORK TOWARDS CROSS-BORDER DATA TRANSFERS

Copyright ©2022

Published on 21st December, 2022

by The Dialogue™

## Authored By

Kamesh Shekar<sup>1</sup>

Ayush Tripathi<sup>2</sup>

Bhavya Birla<sup>3</sup>

Eshani Vaidya<sup>4</sup>

## Edited By<sup>5</sup>

Sreyan Chatterjee

Shruti Shreya

## Designed By

Diksha Kumari

<sup>1</sup>Kamesh Shekar is a Programme Manager - Privacy and Data Governance at The Dialogue. Corresponding author's Email ID: [kamesh@thedialogue.co](mailto:kamesh@thedialogue.co)

<sup>2</sup>Ayush Tripathi is a Programme Manager at The Dialogue.

<sup>3</sup>Bhavya Birla is Research Associate at The Dialogue.

<sup>4</sup>Eshani Vaidya is a Senior Research Associate at The Dialogue.

<sup>5</sup>Sreyan Chatterjee is a Senior Research Consultant at The Dialogue; Shruti Shreya is a Programme Manager at The Dialogue.



## EXECUTIVE SUMMARY

Over the past decade, data has emerged as one of the most valuable economic assets globally. Perhaps for the first time since the industrial revolution, globally countries are on the same footing in terms of their endeavours to extract the maximum possible value from it. Therefore, it is no surprise that countries across the world are trying to institute different data governance frameworks, which would maximize possible opportunities for data utilisation and avenues for its commercialisation within their jurisdictions. However, creating an enabling data flow ecosystem at the global level is not a simple task. Regulations must balance right to individual privacy with economic rights to business entities and develop a holistic approach that combines the two through a more balanced regime. At present, cybersecurity measures are at the most advanced stages of regulation, considering their direct impact on one's individual right to privacy as well as overall data sovereignty.

Secure, trusted, and human rights-friendly technology fosters the sustainable economic growth of the countries, and it requires the free flow of data across national borders to unlock the maximum potential of data for all stakeholders. The free flow of data feeds innovation, economic proliferation, and competition and creates opportunities for MSMEs and start-ups.<sup>6</sup> Realising this potential, recent measures like the European Union's Data Strategy 2020<sup>7</sup>, the United Kingdom's National Data Strategy<sup>8</sup> etc., are actively working towards developing a framework for transferring personal data to international partners wherever appropriate.

Similarly, in the recent iteration of India's Digital Personal Data Protection Bill, 2022 (DPDPB, 2022) the government has relaxed data localisation to introduce trusted data flows to notified countries through clause 17. However, as we move forward, it is critical for the government to establish a standardised procedure for determining the following— (a) countries to which data flow could happen, (b) a framework to be followed for data transfers and (c) mechanisms to be followed for data transfers.

While notifying countries would be one way to facilitate cross-border data transfers, the government needs to consider other existing mechanisms followed by the businesses discussed in Box A. This could bring certainty to business operations and weed out implementational concerns related to cross-border data transfers to the countries where data flows are currently operational. Therefore, as India moves towards enabling cross-border data transfers, it is essential to consider combining existing mechanisms with the discussed principles as a foundation. Embedding principles to the mechanisms would aid in smoothing the friction points with domestic regulations by building consensus and trust.

Against this backdrop, the report discusses the impact of a restrictive approach towards cross-border data transfers. It highlights that adopting a principle-based framework could be one of the best possible options that India could consider, which fulfills the objectives of deploying safeguards to ensure security, privacy and data protection of Indian users while allowing data to flow freely across borders to notified countries. The report builds on how a principle-based framework can act as a foundation on which businesses can follow different data transfer mechanisms as discussed in box A to enable the free flow of data between India and partner countries.

<sup>6</sup> Tripathy, A., Venkatesh, K., & Pande, T. (2021). Impact study: Personal Data Protection Bill on the Startup Ecosystem. Retrieved from The Dialogue: [https://thediologue.co/wp-content/uploads/2021/01/Startup-Report-Final-Documents-vF.pdf?fbclid=IwAR1XJJURqA5EHB\\_IdBpCxEl0TpPlqXbXpzFu8HW7L3R\\_HwZA1eKDq2eDo4](https://thediologue.co/wp-content/uploads/2021/01/Startup-Report-Final-Documents-vF.pdf?fbclid=IwAR1XJJURqA5EHB_IdBpCxEl0TpPlqXbXpzFu8HW7L3R_HwZA1eKDq2eDo4)

<sup>7</sup> A European Strategy for data. (2020). Retrieved from European Commission: <https://digital-strategy.ec.europa.eu/en/policies/strategy-data>

<sup>8</sup> National Data Strategy. (2020). Retrieved from GOV.UK: <https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy>

### Box A: Cross-Border Data Transfer Mechanism

**Adequacy decision:** This mechanism enables the free flow of data to other countries when the respective data protection authority is satisfied that the third country where the data is intended to flow has adequate data protection.

**Cross-Border Privacy Rules (CBPR):** While adequacy decisions at the jurisdiction level formally recognise other countries' data protection regulations to enable the free flow of data, at the business level, we have systems like CBPR. This is a government-provided data privacy certification for data fiduciaries to indulge in cross-border data transfers.

**Market mechanisms:** Various market mechanisms allow data fiduciaries to prove their adequacy and help demonstrate compliance with data protection and privacy safeguards. Some of the prominent mechanisms are

**Certification Schemes:** While CBPR is a government-provided certification, at the market level, data fiduciaries can also certify using government-recognised third-party data protection certification, which acts as a gate pass for cross-border data transfer.

**Codes of Conduct:** This mechanism allows trade associations and other representative bodies to formulate sector-specific guidelines and get them approved by the government. These guidelines are tailor-made to cater to data protection challenges shared by specific sectors or industries.

**Binding Corporate Rules (BCR):** This mechanism provides adequate privacy safeguards for making restricted data transfers within the undertaking of data fiduciaries, franchises and branches, partners etc., which are located outside the country.

**Contractual Clauses:** While BCR is for restricted data transfers like intra-group data exchange, at the border level, data fiduciaries can use contractual clauses mechanism with offshore third-party organisations to transfer data. Using this, data fiduciaries can transfer data across borders by incorporating data protection clauses recognised by the government as part of the contract.

Since data security is agnostic to the location of storage, a principle-based framework approaches this in a more distinct manner by emphasising the importance of having certain minimum technical standards across data lifecycle management as discussed in Box B. This ensures data security irrespective of storage location.

While data protection is approached differently by India and partner countries to cater to their respective domestic concerns and needs, our research on cross-jurisdictional analysis of data protection regulations shows there is potentially a principle-level congruence between India and other leading data protection regimes. Where India's upcoming DPDPB 2022 is advised by some of the key data protection principles like storage limitation, data minimisation, purpose limitation etc.<sup>9</sup> We believe this similarity at the principles level, can act as a means to initiate a conversation between India and partner countries in terms of enabling data flow and digital trade partnerships through consensus building. Therefore, the proposed principle-based framework would bring a nuanced and holistic approach to cross-border data transfer mechanisms within the business-related data transfers (B2B) chain.<sup>10</sup> Moreover, in effect, we intend to use this report to address a gap that exists in practices and strategies for data transfers, which are purpose-based and impacted by domestic legislation.

<sup>9</sup> Explanatory Note - The Digital Personal Data Protection Bill, 2022. (n.d.). MeitY. Retrieved December 16, 2022, from <https://www.meity.gov.in/writereaddata/files/Explanatory%20Note-%20The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf>

<sup>10</sup> The scope of the report is limited to B2B transfers excluding B2G and G2G data transfer chain.

There are various mechanisms (refer to Box A) through which cross-border data transfers happen for business-related data transfers, subject to the entity’s nature. However, the framework proposes a systematic way to approach cross-border data transfer mechanisms, where principles discussed in this report will be a prerequisite for various kinds of business-to-business data transfer chains, i.e., data fiduciaries to data fiduciaries, data fiduciaries to data processors and data fiduciaries to data storage facilities. For the purpose of this report, we discuss various principles across the data lifecycle, bucketed and mapped to respective players within the data ecosystem (refer to Figure A). While there are various players involved within the data ecosystem, for this report, we cover four key players, i.e., data fiduciaries, intermediaries, data processors and data centres. Additionally, this paper also discusses principles for regulators/governments such that implementing a principle-based framework is seamless.

The principles discussed, across this report, are the key universal and internationally recognised data protection and design principles (refer to Box B) embedded in various cross-border data transfer arrangements and data protection regulations across jurisdictions, including India.

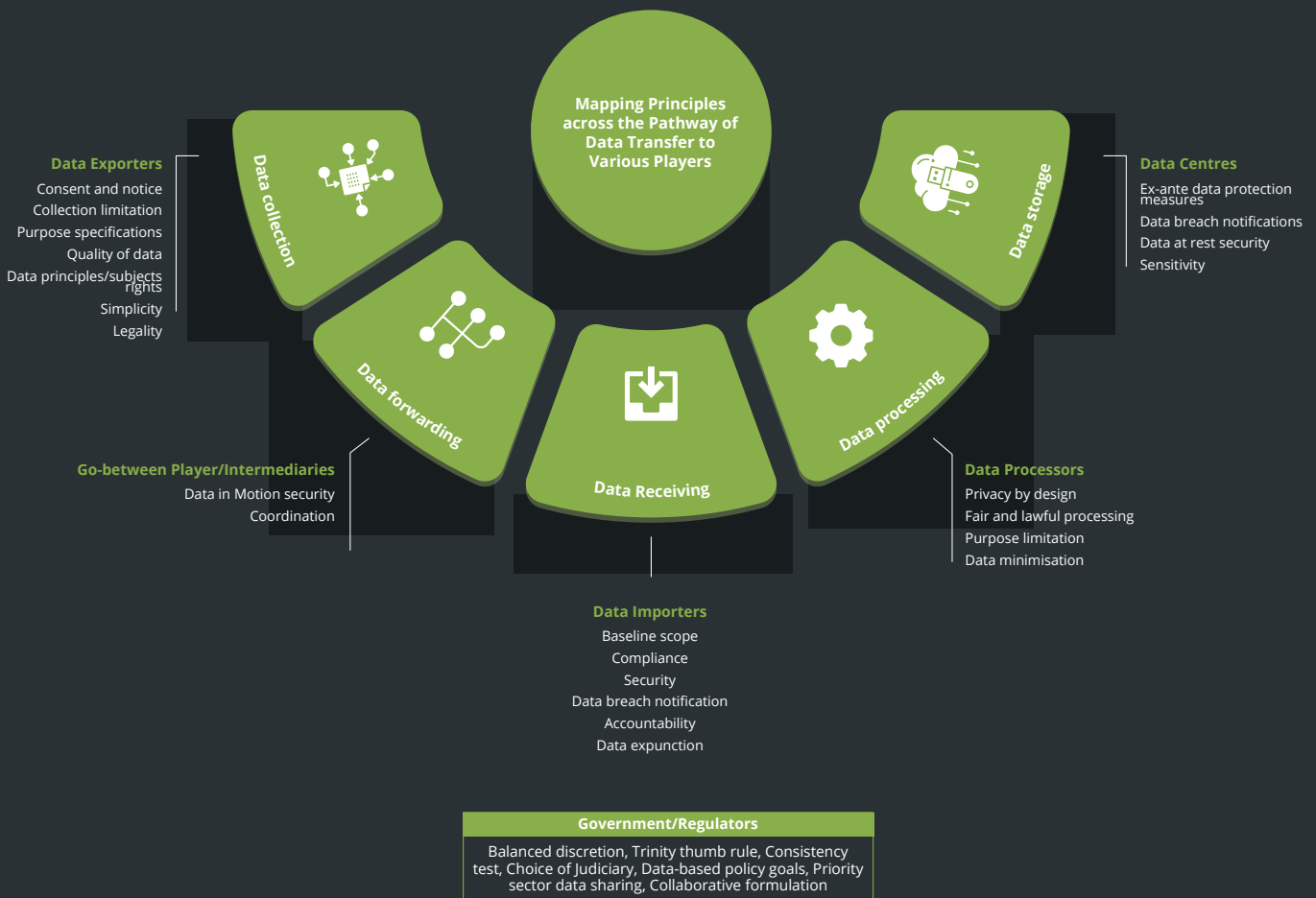


Figure A

### Box B: Principle-based Framework for Data Transfers

**Principles for Data Exporters:** Data fiduciaries collect information about consumers, directly by seeking information from individuals and indirectly through third parties etc. However, the focus of business-related cross-border data transfers has been mainly on data which is directly collected from individuals. As it is futile to differentiate data based on transfers, the principles such as consent and notice, collection limitation, purpose specifications, quality of data, data principals/subject's rights, simplicity, and legality must be at a broader level of data collection done by data exporters with some specifics to cross-border data transfers.

**Principles for Data Importers:** On receiving data from data exporters, the data importers must ensure the data received is treated with as much protection as what it was treated in the home country. Data importers must have reasonable measures to ensure the data received is not misused. Reasonable measures must be advised by principles such as baseline scope, compliance, security, data breach notification, accountability, and data expunction embedded.

**Principles for Data Processors:** Both data exporters and data importers process data for providing services to data principals, betterment of service delivery, marketing purposes, competition purposes etc. While processing of data by data exporters comes under the purview of the regulations of their home country, the principles such as Privacy by Design, fair and lawful processing, purpose limitation, and data minimisation must be followed by third parties, data processors and cloud service providers who are stationed in other jurisdictions.

**Principles for Data Centres:** Data fiduciaries store data offshore on the cloud or on physical servers, as most data centres are located in the United States, United Kingdom, Germany etc. Data centre's biggest threat at the storage stage is breaches through hacking, leaks, etc. Data breaches result in a reputational loss for data exporters who have stored their data offshore. In addition, data exporters are likely to face heavy fines from domestic regulators and could be barred from indulging in cross-border data transfers. Thus, data exporters have to exercise their oversight to ensure that the data centres which store the data offshore follow principles such as ex-ante data protection measures, data breach notification, data at rest security and data sensitivity.

**Principles for Go-Between Player/Intermediaries in Data Transfers:** Cross-border data transfers involve data exporters and data importers, data processors and data centres at the ends. However, as data gets forwarded to a third country, there are two key go-between players/intermediaries, i.e., connectivity providers and internet service providers. While most of the models and mechanisms are concerned with end players, through this principle-based framework, we take a holistic approach towards cross-border data transfers where the principles such as data in motion security, coordination, data anonymity commend go-between players' compliance.

**Principles for Government/Regulators:** Implementing the principle-based framework for cross-border data transfers will require a concerted effort, in terms of coordination and cooperation. The zero step towards implementing the principle-based framework would require domestic stability with regards to data protection regulations. However, there are also various other roadblocks to implementing the principle-based framework for cross-border data transfer, which cannot be solved exclusively at a domestic level. A concerted effort is needed between the signatory jurisdictions beyond its borders to increase data flow. Some of the key principles to be considered by the domestic regulators and governments in enhancing international-level coordination and cooperation are: balanced discretion, trinity thumb rule, consistency test, choice of jurisdiction, data-based policy goals, collaborative formulation, and recognition of accountability principle.



Therefore, as India moves toward enabling cross-border data transfers through various means (refer to Box C) with other notified jurisdictions, we believe it is essential to consider a combination of data transfer mechanisms, as discussed in this report, tailored to embed the principles discussed as part of the overarching framework. This was also emphasised by start-ups and cloud service providers, about 84% of our respondents expressed the need for a principle-based framework to enable cross-border data transfers and ease of compliance.

### Box C: Implementational Roadmap for a Principle-Based Data Transfer Framework

Coordination of various factors is essential for the seamless implementation of the principle-based data transfer mechanism. This section will explore the foundations for enhancing the digital economy partnership between India and other jurisdictions by adopting a principle-based data transfer framework. While there are various means through which India can adopt a principle-based data transfer framework, there are three key means:

**Statutory Mechanisms:** As India is yet to establish a data protection regime and is currently drafting the same, it is ideal to have a principle-based data transfer framework with room for updating principles provisioned within it or through subsequent subordinate legislations. A combination of the mechanisms discussed in Box A must be provisioned within the bill or through subsequent subordinate legislations such that it is tailored to embed the principles discussed in Box B.

**Bilateral Agreements:** There are various existing and upcoming bilateral arrangements between India and other jurisdictions. India must use existing/upcoming arrangements to establish and enable principle-based data transfers. While enabling cross-border data transfers is overwhelmingly beneficial, it is more lucrative to enable it with countries which share a positive relationship in trade, investments etc. Therefore, though there are various bilateral arrangements, some of the key bilateral arrangements with key jurisdictions like the United States, Australia, the United Kingdom, UAE, Japan, and Singapore, must be enhanced to establish a principle-based framework for data transfers.

**Multilateral Arrangements:** There are various existing multilateral frameworks (both binding & non-binding) that India can utilise to introduce principle-based data transfer mechanisms. The arrangements must include agreements, strategies, and declarations to which India is currently a signatory, as well as arrangements to which India could potentially consider being a signatory in future for enabling the free flow of data.


In addition to adopting a principle-based framework, we suggest both India and other jurisdictions must aid businesses in implementing principles (irrespective of mechanisms they choose) within their procedures and processes by forming various operational guidelines, SOPs, awareness programs, and private consultations. These aiding materials prepared by the governments must be tailored according to the domestic context and socio-economic-political fabric that the businesses are working within for seamless implementation. Moving forward, it is also crucial to identify a government agency with enforcement authority to supervise procedures and processes of businesses to monitor alignments with principles through mechanising various soft and hard enforcement measures. Also, enforcement measures must be evaluated and implemented according to the nature and size of the non-compliance.





# TABLE OF CONTENTS

<b>1. INTRODUCTION</b>	<b>01</b>
1.1. Research Methodology	02
1.1.1. Secondary Research	02
1.1.2. Primary Research	03
<b>2. GLOBAL DATA PROTECTION LANDSCAPE</b>	<b>05</b>
2.1. Asia	06
2.2. Africa	06
2.3. South America	07
2.4. North America	07
2.5. Europe	07
2.6. Oceania	08
<b>3. IMPACT OF RESTRICTING CROSS-BORDER DATA TRANSFERS</b>	<b>09</b>
3.1. Impact On Data Processors/Cloud Service Providers	09
3.1.1. Differential Economic Impact	10
3.1.2. Implementation Concern	11
3.2. Impact On Start-Ups	11
3.2.1. Direct And Indirect Impact	12
3.2.2. Regulatory Uncertainty	12
3.2.3. Operational Concern	13
<b>4. PRINCIPLE-BASED FRAMEWORK FOR DATA TRANSFERS</b>	<b>15</b>
4.1. Data Fiduciary Data Transfers	17
4.1.1. Principles For Data Exporters	21
4.1.2. Principles For Data Importers	22
4.2. Principles For Data Processors	23
4.3. Principles For The Data Centre	24
4.4. Principles For Go-Between Player/Intermediaries In Data Transfers	25
4.5. Principles For Government/Regulators	26



<b>5. IMPLEMENTATIONAL ROADMAP FOR A PRINCIPLE-BASED DATA TRANSFER FRAMEWORK</b>	<b>31</b>
5.1. Statutory Mechanism	31
5.2. Trade Arrangements	33
5.2.1. Multilateral Arrangements	33
5.2.2. Bilateral Arrangements	35
<b>6. PRIORITY AREAS FOR GOVERNMENTAL NEGOTIATION</b>	<b>39</b>
6.1. Interoperable Data Protection Regime	40
6.2. Minimalistic Compliance Regime	41
<b>7. CONCLUSION</b>	<b>43</b>
<b>8. ANNEXURE 1</b>	<b>45</b>
<b>9. ANNEXURE 2</b>	<b>47</b>

# 1. INTRODUCTION

Technological developments are increasingly moving toward data-driven business models which aim to value data in economic terms. In the wake of data commercialisation, States have tried to enact robust data production regulations to protect user rights. While these attempts try to secure the data, the recent developments like the EU's Data Strategy 2020<sup>11</sup>, UK's National Data Strategy<sup>12</sup>, etc., are actively working towards developing a framework for transferring personal data to international partners wherever appropriate. Simultaneously, we see attempts made by States, as discussed in this paper, to institute data sovereignty<sup>13</sup> rules that would give them the maximum possible opportunities over data and avenues for its commercialisation within their jurisdictions.

In this report, we show how data localisation doesn't translate into sustainable economic development and enhance security but rather impacts the businesses like cloud service providers and start-ups which are less discussed within the data localisation literature.

There are three forms of data transfer chains depending upon the purpose for which the data is shared, i.e., (a) the data transfer for fulfilling contractual duties and for business purposes which happens between business to business, data transfer for the legal enforcement purpose which happens between (b) businesses to government (c) government to government. As of now, the players in these data transfers chain use various mechanisms for cross-border data transfers. For instance, the Cross-Border Privacy Rules of Asia-Pacific Economic Cooperation (APEC)<sup>14</sup> for business transfers, and mechanisms like Mutual Legal Assistance Treaty (MLAT)<sup>15</sup>, Clarifying Lawful Overseas Use of Data Act (CLOUD Act)<sup>16</sup> etc., are used for law enforcement-related data transfers.

While these mechanisms take various approaches toward cross-border data transfers, they are not holistic in nature, and many of these mechanisms hit a roadblock when they face friction with domestic regulations. Therefore, to address this literature gap, we propose a principle-based data transfer framework that brings a nuanced and holistic approach to cross-border data transfer mechanisms within the B2B data transfer chain.<sup>17</sup> Moreover, the principles proposed in our research report would aid India and other jurisdictions in collaboratively determining data protection levels. In effect, we intend to use this report to address a gap that exists in practices and strategies for data transfers, which are purpose-based and get impacted by domestic legislation.

<sup>11</sup> A European Strategy for data. (2020). Retrieved from European Commission: <https://digital-strategy.ec.europa.eu/en/policies/strategy-data>

<sup>12</sup> National Data Strategy. (2020). Retrieved from GOV.UK: <https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy>

<sup>13</sup> Bertucci, D. (2022, April 5). What Is Data Sovereignty? Ultimate Guide | Auvik. Auvik Networks. Retrieved December 20, 2022, from <https://www.auvik.com/franklyit/blog/data-sovereignty-everything-you-need-to-know/>

<sup>14</sup> APEC Cross-border Privacy Enforcement Arrangement (CPEA) | APEC. (n.d.). Asia-Pacific Economic Cooperation. Retrieved August 9, 2022, from <https://www.apec.org/groups/committee-on-trade-and-investment/digital-economy-steering-group/cross-border-privacy-enforcement-arrangement>

<sup>15</sup> <https://legalaffairs.gov.in/documents/mlat>

<sup>16</sup> Goldman, B. (2018, April 6). *The CLOUD Act, Explained*. Orrick. Retrieved August 9, 2022, from <https://www.orrick.com/en/Insights/2018/04/The-CLOUD-Act-Explained>

<sup>17</sup> The scope of the report is limited to B2B transfers excluding B2G and G2G data transfer chain.

Section 1.1 discusses the research methodology, followed by which Chapter 2 summarises the policy directions that jurisdictions are taking toward cross-border data transfers. The section clusters various jurisdictions into the degree of restrictiveness of cross-border data transfers. Chapter 3 discusses the impact of the restrictive cross-border data transfers and data localisation on data processors, cloud service providers and start-ups. Chapter 4 discusses the need for a uniform set of principles and criteria that could aid India in determining the levels of data protection collaboratively with other jurisdictions for business-related data transfers (B2B). Chapter 5 discusses various ways in which India and other jurisdictions can enable principle-based cross-border data transfers. Finally, chapter 6 discusses some of the priority areas in the digital environment to be negotiated at the governmental level to (a) secure human rights, labour rights, digital inclusion and equity, and (b) have the least restrictive cross-border data protection at the domestic level.

## 1.1. RESEARCH METHODOLOGY

The study adopted a two-pronged approach in terms of methodology involving both secondary research and primary research. This section will discuss the details of the methodology in terms of research design, sampling size, time span etc., of the study.

### 1.1.1. SECONDARY RESEARCH

The study undertook a detailed meta-analytic literature review to understand the data protection regulation landscape and mechanisms followed in other jurisdictions to outline the policy direction that India can take to enable data transfers between other jurisdictions. Our literature review covers the following aspects.

**Global data protection landscape:** We analysed various approaches countries have taken in their data regulations covering (a) Asian countries like India, China, Japan, Singapore, Philippines, Thailand, South Korea, and Bangladesh, (b) European countries like EU, Russia, UK (c) North American countries like the US, Mexico, Canada (d) South American countries like Brazil, Argentina, Columbia (e) African countries like South Africa, Rwanda, Ghana, Kenya, Morocco, Uganda (f) Oceania countries like Australia, New Zealand. (refer to Annexure 1)

**Existing cross-border data transfer mechanism:** Our literature review also covered analysing existing cross-border data transfer mechanisms such as the Regional Comprehensive Economic Partnership, APEC - CBPR, UK's post-Brexit data transfer arrangement, OECD Guidelines on the protection of privacy, ASEAN Model Contractual Clauses, ASEAN Data Sandbox (GSMA), World Economic Forum's data protection principles etc.

**Bilateral and Multilateral Agreement:** Finally, our research also analysed the existing and upcoming bilateral and multilateral agreements between India and other jurisdictions to lay out the implementation roadmap for the principle-based cross-border data transfers framework (discussed in chapter 4). Some of the key multilateral agreements analysed are the Indo-Pacific Strategy, QUAD,

Joint Declaration on privacy and the protection of personal data, Data Free Flow with Trust framework, Joint Initiative on E-commerce, and G20 Leader's Riyadh Declaration. Some of the bilateral agreements analysed are the Indo-US Bilateral Arrangement, Australia-India Comprehensive Economic Cooperation Agreement (in negotiations), India-UK Free Trade Agreement (in negotiations), Indo-UAE Federal Trade Agreement (recently concluded), Indo-Japan Comprehensive Economic Partnership Agreement, and Indo-Singapore Comprehensive Economic Partnership Agreement.

## 1.1.2. PRIMARY RESEARCH

The study is based on primary research with inputs from industry stakeholders from India to understand multiple viewpoints and concerns around restricting cross border data flows. As tabulated below, we received 25 inputs from various stakeholders, predominantly from start-ups and cloud service providers/data processors.

Stakeholder type	Participant number
Start-ups	19
Cloud Service Providers/ Data Processors	6

The study took an interpretivist lens by adopting a qualitative research approach to observe the impact of the data localisation and restrictive cross-border data transfers on cloud service providers, data processors and start-ups. Besides, the research conducted for this study was deductive in nature, where we analysed the impact the data localisation and restrictive cross-border broader data transfers using secondary research and moved towards building upon those inferences with data collected through primary research.

In the span of three months (May 2022 - August 2022), we collected data for this study in a cross-sectional time horizon manner where all the needed input from the respondents was collected at one point in time with occasional follow-ups. Some of the key details about our primary research methodology, starting from the sampling strategy to the analysis technique adopted for this study, can be found in Annexure 2.





## 2. GLOBAL DATA PROTECTION LANDSCAPE

The number of data protection regulations enacted by jurisdictions has been steadily increasing over the last decade, with 137 countries having data protection laws as of December 2021.<sup>18</sup> These legislations have amalgamated global best practices and incorporated them into laws that align with their respective domestic policy goals and realities, emanating from the European Union General Data Protection Regulation's (EU GDPR) principle-based approach that has been widely used as foundational legislation for countries to develop.

Post the COVID-19 pandemic, our reliance on digital services has compounded, as has been studied specifically in the case of India<sup>19</sup> as well as globally. These trends establish the need for research in this domain as data trade restrictions can fundamentally alter a jurisdiction's economic standing globally and affect consumer behaviour with technologies that have become ubiquitous over the pandemic.

This chapter maps the various approaches the countries take, emphasising decisions on the restrictiveness of data transfers between countries. We have approached this assessment through a thorough analysis of local regulations and clustered various jurisdictions (within the continents) into the degree of restrictiveness of cross-border data transfers. A country-wise breakdown of data localisation policies is added to Annexure 1 and can be referred to in complement to the analysis provided in this chapter for a holistic perspective.

Data flow restrictions have nearly doubled over the last five years. In 2017, 35 countries implemented 67 such barriers, and there are two kinds of data flow restrictions, as discussed in box 1 in the next chapter.<sup>20</sup> By mid-2021, 62 countries had imposed 144 cross-sectoral data flow restrictions, while dozens more are under consideration both at a country level and even at regional levels.<sup>21</sup> The total number of data localisation policies (explicit and *de facto*) has more than doubled from 67 in 2017 to 144 in 2021. Another 38 data localisation policies have been proposed or considered in countries worldwide. Amongst these countries, China (29), India (12), Russia (9), and Turkey (7) stand the highest in terms of requiring forced data localisation. Following is the continent-wise analysis of data protection regulations.<sup>22</sup>

<sup>18</sup> United Nations Conference on Trade and Development (2021 December 14) *Data Protection and Privacy Legislation Worldwide*, (Online) retrieved from <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

<sup>19</sup> De, R., Pandey, N. & Pal, A. (2020 June 9) *Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice*, Elsevier Public Health Emergency Collection - PMC7280123. Retrieved on June 21, 2022 from <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7280123/>

<sup>20</sup> Cory, N. & Dascoli, L. (2021 July 19) *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, Information Technology and Innovation Foundation (ITIF). Retrieved on June 23, 2022 from <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>

<sup>21</sup> Ibid.

<sup>22</sup> Ibid.

## 2.1. ASIA

One of the main challenges to cross-border data transfer in Asia is the fragmented and varying national requirements regarding the use of personal data. Asia is home to the largest number of countries imposing or considering to impose data localisation mandates. Asia is also home to 3 of the top 5 most restrictive countries when it comes to cross-border data flows (China, Indonesia and Vietnam).<sup>23</sup> The region also presents an incongruence between industry realities and policymaking. As Asia (particularly East Asia) is home to most small businesses in the world that are reliant on the internet, the data flows become key for their functioning. Even their contribution to national GDP is significant, between 35-70% of the revenue generated.<sup>24</sup> Small businesses also account for 60-98% of all businesses and 50-98% of employment in certain countries.<sup>25</sup> Therefore, enabling the free flow of data across borders becomes crucial for the continent, as any bottlenecks are bound to have significant economic impacts. While the continent as a whole tends to move towards data nationalism, certain countries like Japan have become part of Free Trade Agreements (FTAs) with other nations such as the United States of America<sup>26</sup> and have also gained adequacy status from the EU.<sup>27</sup>

## 2.2. AFRICA

30 countries in Africa (54% of African countries) have specific data protection laws, with eight others (17% of African countries) in the process of drafting data protection legislation. 16 countries still don't have any data protection laws in place.<sup>28</sup> Africa has been evenly split when it comes to data localisation mandates, with 26 countries with no data flow restrictions and 26 with conditional data flow mandates in place.<sup>29</sup> Multiple African nations also impose sectoral data localisation mandates for financial services (Nigeria, Ethiopia, Rwanda and Uganda), cybersecurity and cybercrimes (Rwanda, Zambia and Zimbabwe), telecommunications (Cameroon, Rwanda and Nigeria) and data protection (Kenya, South Africa, Tunisia and Uganda) laws to place restrictions on cross-border transfer of data, with the data transfer permitted where certain conditions are met, or where authorisation is granted by the relevant government bodies before the cross-border transfer is allowed.<sup>30</sup>

<sup>23</sup> Ferracane, M.F., Makiyama, H.L. & Van der Marel, E. (2018 May) *Digital Trade Restrictiveness Index*, European Centre for International Political Economy. Retrieved on June 23, 2022 from [https://ecipe.org/wp-content/uploads/2018/05/DTRI\\_FINAL.pdf](https://ecipe.org/wp-content/uploads/2018/05/DTRI_FINAL.pdf)

<sup>24</sup> Asia Cloud Computing Association (2015) *SMEs in Asia Pacific: The market for Cloud Computing*. Retrieved on August 7, 2022 from <https://www.slideshare.net/acccloud/smes-in-asia-pacific-the-market-for-cloud-computing-case-studies-of-14-markets-in-apac-227579703>

<sup>25</sup> Ibid.

<sup>26</sup> USTR (2019) *Agreement between the United States of America and Japan concerning Digital trade*. Retrieved on August 9, 2022 from [https://ustr.gov/sites/default/files/files/agreements/japan/Agreement\\_between\\_the\\_United\\_States\\_and\\_Japan\\_concerning\\_Digital\\_Trade.pdf](https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf)

<sup>27</sup> European Commission (2019 January 23) *European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows*. Retrieved on August 10, 2022 from [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_19\\_421](https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421)

<sup>28</sup> Quaye, T. (2021 January) *Africa's Data Opportunity? Cross-border data flows and IOT*, Smart Africa. Retrieved on August 3, 2022 from <https://www.gsma.com/publicpolicy/wp-content/uploads/2021/01/Africas-Data-Opportunity-Cross-Border-Data-Flows-and-IoT-Webinar-Slides.pdf>

<sup>29</sup> Mbugua, C. (2021 January) *Africa's Data Opportunity? Cross-border data flows and IOT*, GSMA. Retrieved on August 3, 2022, from <https://www.gsma.com/publicpolicy/wp-content/uploads/2021/01/Africas-Data-Opportunity-Cross-Border-Data-Flows-and-IoT-Webinar-Slides.pdf>

<sup>30</sup> Abinallah, A. et al. (2021 November) *Mapping and Analysis of Privacy Laws in Africa*, The Collaboration on International ICT Policy in East and Southern Africa (CIPESA). Retrieved on August 5, 2022, from [https://cipesa.org/?wpfb\\_dl=479](https://cipesa.org/?wpfb_dl=479)

## 2.3. SOUTH AMERICA

South America is home to a largely homogenous stance on data localisation as most countries have adequacy standards to be fulfilled for international data transfers to occur. The continent has Argentina and Uruguay, both of whom have adequacy status from the EU<sup>31</sup> and Colombia, which imposes an adequacy standard of its own that is not as intensive as GDPR but inspired by it and mandates that data processors be registered with its Data Protection Authority.<sup>32</sup> Brazil, too imposes adequacy measures under Chapter V of its Data Protection Law.<sup>33</sup>

## 2.4. NORTH AMERICA

The North American region, i.e., the United States of America, Canada and Mexico, follow either adequacy standards or no bars on the free flow of data to and from the continent. The United States of America<sup>34</sup> has entered into FTAs for digital trade with multiple countries in order to achieve the same as well.

For instance, the United States-Mexico-Canada trade agreement (USMCA) is the primary digital trade instrument in place that enables cross-border data to flow between North American countries. However, Mexico still implements data localisation for financial data while other nations in the region also have sectoral data localisation norms in place.<sup>35</sup> Bills in the Canadian Parliament, namely the Digital Charter Implementation Act of 2022<sup>36</sup> if adopted by Parliament, would repeal parts of the Personal Information Protection and Electronic Documents Act (PIPEDA) and enact a new Consumer Privacy Protection Act and a new Personal Information and Data Protection Tribunal Act (PIDPTA).

## 2.5. EUROPE

Europe has been at the forefront of building jurisprudence around data protection, whose GDPR serves as a foundational document for countries to model their data protection laws in tandem. While the EU relies on adequacy standards to be fulfilled for data transfers to take place and has perhaps the strictest requirements, outlining the need for societal features such as the precedence of ‘the rule of law’ and respect for human

<sup>31</sup> European Commission, Adequacy Decisions. Retrieved on August 9, 2022 from [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)

<sup>32</sup> CMS (2021 February 18) Data Protection and Cybersecurity Laws in Colombia. Retrieved on August 7, 2022 from <https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/colombia>

<sup>33</sup> Rodriguez, K et al. (2020) The State of Communication Privacy Law in Brazil, Electronic Frontier Foundation. Retrieved on August 9, 2022 from <https://necessaryandproportionate.org/uploads/2020-brazil-en-faq.pdf#question4>

<sup>34</sup> Fact Sheet: Key Barriers to Digital Trade | United States Trade Representative. (n.d.). USTR. Retrieved December 19, 2022, from <https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2016/march/fact-sheet-key-barriers-digital-trade>

<sup>35</sup> McNees, J. & Smith, S. (2021) National Trade Estimate Report on Foreign trade barriers, USTR. Retrieved on August 8, 2022 from <https://ustr.gov/sites/default/files/files/reports/2021/2021NTE.pdf>

<sup>36</sup> Parliament of Canada (2022 June 16) An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, C-27. 1st Session of the 44th Parliament. Retrieved on August 9, 2022 from <https://www.parl.ca/legisinfo/en/bill/44-1/c-27>

rights for jurisdictions to be deemed adequate, the European Data Protection Board (EDPB) has been in continuous consultations to make adequacy standards tougher.<sup>32</sup>

Similarly, in Russia, cross-border data flows are allowed, but there are *de-facto* localisation norms in place as there are no bars on the transfer of data outside the country, but the collection and storage of the same have to be in Russia. Granting remote access to databases located in Russia from the territory of another country is not prohibited under Federal Law 242-FZ.<sup>33</sup>

## 2.6. OCEANIA

Australia doesn't mandate data localisation at a federal level, but sectoral regulations that cover health and financial data, have data localisation mandates in place. Australia has one of the stringent health data localisation norms in the world that do not allow the transfer of health data outside the country.<sup>39</sup> The country also mandates that cloud service providers storing land information under the Electronic Conveyance National Law must store the data in Australia.<sup>40</sup> Under the Australian Privacy Principles (APP), the transfer of personal data outside of Australia is allowed as long as the APPs permit.

New Zealand ranks the lowest in the Data Trade Restrictiveness Index as the country enables the free flow of data and only applies the necessary amount of obligations to be fulfilled before data can be transferred outside the country. The country also has adequacy status to trade with the EU and maintains its own version of the EU's 'essential equivalence' list of countries.<sup>41</sup> Cross-border data flows in the country are regulated by their Information Privacy Principles (IPP), more specifically principle 12, which lists six grounds out of which one needs to be satisfied for data to be transferred out of New Zealand.

<sup>37</sup> EDPB (2020 February) Recommendations 02/2020 on the European Essential Guarantees for surveillance measures. Retrieved on August 9, 2022 from [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_recommendations\\_202002\\_europeanessentialguaranteessurveillance\\_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf)

<sup>38</sup> KPMG (2018) The 'Localisation' of Russian citizens' personal data. Retrieved on August 9, 2022 from <https://assets.kpmg/content/dam/kpmg/be/pdf/2018/09/ADV-fact-sheet-localisation-of-russian-personal-data-uk-LR.pdf>

<sup>39</sup> Parliament of Australia (2017 September 20) My Health Records Act, 2012. Retrieved on August 8, 2022 from <https://www.legislation.gov.au/Details/C2017C00313>

<sup>40</sup> ARNECC, Electronic Conveyancing National Law. Retrieved on August 7, 2022 from [https://www.arnec.gov.au/regulation/electronic\\_conveyancing\\_national\\_law/#:~:text=The%20Electronic%20Conveyancing%20National%20Law,of%20National%20Law\)%20Act%202012](https://www.arnec.gov.au/regulation/electronic_conveyancing_national_law/#:~:text=The%20Electronic%20Conveyancing%20National%20Law,of%20National%20Law)%20Act%202012)

<sup>41</sup> European Commission (2012 December 19) Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand (notified under document C(2012) 9557) Retrieved on August 9, 2022 from <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013D0065>

## 3. IMPACT OF RESTRICTING CROSS-BORDER DATA TRANSFERS

The United Nations Conference on Trade and Development (UNCTAD) noted that 2020 saw the most significant one-year rise in internet traffic (35%) since 2013, owing to the pandemic and the push to go digital in order to continue functioning.<sup>42</sup> The report also established that around 80% of all internet traffic is related to social media, gaming and video streaming.<sup>43</sup> These trends thus establish our growing reliance firstly on the internet and secondly on the cross-border data flows that enable our access to websites hosted through servers across the globe.

While there is much general discussion on data localisation, this chapter discusses how it affects data processors, cloud service providers, and start-ups. The chapter also discusses the practical implementation problems to be faced by data processors, cloud service providers, and start-ups. In addition to our secondary research, in this chapter, we have inferences from inputs received from industry stakeholders such as data processors, cloud service providers, and start-ups.

### 3.1. IMPACT ON DATA PROCESSORS/ CLOUD SERVICE PROVIDERS

While there can be various considerations behind data localisation by regulators and legislators, one of the key rationales of the government behind data localisation is to secure the data of individuals, i.e., considering data is more private and secure if stored within the country. However, research proves that data localisation doesn't translate into high commercial privacy and data security standards.<sup>44</sup> Additionally, our research<sup>45</sup> unpacks the security paradox of data localisation, where we highlight that the security of data is not a function of where it is stored. Besides, as many business entities have a "legal nexus"<sup>46</sup>, they can't escape a nation's regulatory mandate despite storing data overseas. Data security and privacy are agnostic to the location of the data server and dependent on the principles and standards (discussed in chapter 4) that the cloud servers or other data centres follow.

<sup>42</sup> *New approach needed to make digital data flow beneficial for all.* (2021, September 29). UN News. Retrieved August 3, 2022, from <https://news.un.org/en/story/2021/09/1101542>

<sup>43</sup> Ibid.

<sup>44</sup> Castro, D. (n.d.). *The False Promise of Data Nationalism.* Itif. Retrieved June 20, 2022, from <https://www2.itif.org/2013-false-promise-data-nationalism.pdf>

<sup>45</sup> Rizvi, K., & Venkatesh, K. (2020, December 23). *Outlook 2021: Designing data governance policies to promote domestic startups.* TechCircle. Retrieved June 26, 2022, from <https://www.techcircle.in/2020/12/23/designing-data-governance-policies-to-promote-domestic-startups>; Venkatesh, K. (n.d.). *Industry Concerns over the Personal Data Protection Bill 2019.* The Dialogue. Retrieved June 26, 2022, from <https://secureservercdn.net/160.153.137.218/3mv9da.myftpupload.com/wp-content/uploads/2021/12/Primer-Business-Implications.pdf>; *Impact Study: Personal Data Protection Bill On The Start-up Ecosystem.* (2021, January 6). The Dialogue. Retrieved June 26, 2022, from <https://thediologue.co/wp-content/uploads/2021/01/Startup-Report-Final-Documents-vF.pdf>

<sup>46</sup> Cory, N. (n.d.). *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?* Itif. Retrieved June 20, 2022, from <https://www2.itif.org/2017-cross-border-data-flows.pdf>

Therefore, it is imperative to strengthen one of the key enablers of cloud service sector export, i.e., cross-border data transfers. Since processing requires the transfer of data at a large scale to deliver the contractual mandate of data fiduciaries, which is an integral element of data processors and cloud service providers' business models. Besides, it would be ideal for the government to aid businesses to seamlessly serve their legal business contract efficiently, which would, in turn, contribute to the economy directly or indirectly.

On the other hand, data localisation and restrictive cross-border data transfers, might have the following impact on the data processors and cloud service providers, which is echoed by the businesses.

### 3.1.1. DIFFERENTIAL ECONOMIC IMPACT

The impact of restricting data transfers would be felt by all sizes of processors and cloud service providers, from start-ups to MNCs, who process data for the data fiduciaries. However, during our stakeholder interviews, most cloud service providers and industry experts expressed that the level of the economic impact to be felt by processors/cloud services would be subject to the customer base of the businesses and the location of the businesses.

**Indigenous processors and cloud service providers:** Indigenous processing and cloud service providers might face a positive impact as fiduciaries might shift their data processing activity to India. However, industry experts said that this positive impact is only for the short-term, whereas in the long term, as the opportunity cost of the same would be high, the country might lose out on the comparative advantage. For instance, if any X country produces bananas efficiently and Y country produces apples efficiently, both countries could forego producing apples and bananas respectively and indulge in trade exchange of these products. Similarly, in this scenario, considering the transfer of data for processing to other countries (which efficiently does it) garners the benefits from better processing capacity.

**Multinational processors/cloud service providers:** Also, industry experts noted that the impact would be disproportionate on emerging cloud service providers as multinational processors and cloud service providers find a fix as they might have a business operation to the country where the data localisation is enacted. However, some multinational processor/cloud service providers noted that localisation could cause intra-operational concerns, increasing the cost of providing services.

### 3.1.2. IMPLEMENTATION CONCERNS

The provisions related to the intra-group scheme<sup>47</sup> are removed from the Digital Personal Data Protection Bill 2022, adding to the concerns expressed by the data processors and cloud service providers. In addition, there is less clarity on factors and parameters to be considered to notify countries to which data can flow and terms and conditions for the data flow. This uncertainty causes concerns to cloud service providers in terms of business planning.

While notifying countries would be one way to facilitate cross-border data transfers, the government needs to consider other existing mechanisms followed by the businesses like BCR, Contractual Clauses, certification mechanisms etc., discussed in this report. This could bring certainty to business operations and weed out implementational concerns related to cross-border data transfers to the countries where data flows are currently operational.

#### Key insights

- Many cloud service providers and industry experts expressed that the level of the economic impact to be felt by processors and cloud service providers would be subjected to the customer base of the businesses and the location of the businesses.
- Industry experts noted that the positive impact faced by the indigenous cloud service providers with data localisation might be only for the short term.
- Emerging cloud service providers noted that they would be disproportionately impacted.
- Some multinational cloud service providers noted that localisation could cause intra-operational concerns, increasing the cost of providing services.
- Cloud service providers noted less clarity on whether the intra-group scheme applied to them could cause an implementational roadblock.

## 3.2. IMPACT ON START-UPS

Implementation of severe data localisation mandates, can hamper the supply of reliable datasets. Also, it may cause other jurisdictions to respond with policy reciprocity with regard to localisation mandates causing catastrophic implications for start-ups as a whole and AI-solutions start-ups in particular. Start-ups voiced various concerns with data localisation during our stakeholder interviews. Some of these concerns are as follows.

<sup>47</sup> Intra-group Schemes Definition. (n.d.). Law Insider. Retrieved December 20, 2022, from <https://www.lawinsider.com/dictionary/intra-group-schemes>

### 3.2.1. DIRECT AND INDIRECT IMPACT

Start-ups pointed out that they may experience both direct and indirect impact of data localisation depending upon the nature of the businesses.

**Direct impact:** They pointed out some direct economic impacts like when it comes to implementation, they have to find (a) an additional layer of money needed on top of other compliance costs and pressure to sustain (b) resource constraints in terms of finding people etc. While some start-ups pointed out that there might be minimal macroeconomic repercussions, at the business level, they noted that the spending on homegrown technological infrastructure might get costlier for them.

**Indirect impact:** Some start-ups pointed out that the cost of data localisation is not always the economic cost, and it involves indirect costs which can't be quantified, like expertise and time. For instance, one of the start-ups pointed out that in a resource-constrained environment, the indirect cost involves lost time in business development and innovation while concentrating on compliance.

On the other hand, they pointed out that budgeting is essential for businesses, and direct and indirect costs (like infrastructure costs) are involved. The direct cost was pointed as costs which increase with customer base rise, which they keep around 50-60% and the rest of the money they spent on indirect costs. As indirect costs increase with data localisation in terms of infrastructure costs etc., start-ups noted that the price of the services and commodities provided would increase, ultimately hampering the demand curve as India is a price-sensitive market. For instance, the Indian market is susceptible to price. Hence, some start-ups pointed out that such sensitivity would further corner them to take on the additional compliance burdens and costs associated with the localisation mandate.

Besides, one of the offshore start-ups noted that if they know that other countries provide a better regulatory landscape where direct and indirect costs are minimal, they may choose to establish a base there for better business outcomes.

### 3.2.2. REGULATORY UNCERTAINTY

It's been five years since the Supreme Court of India recognised privacy as a fundamental right placing a positive obligation on the government to enact data protection regulations.<sup>48</sup> Since then, there have been many versions of data protection bills. Start-ups pointed out that uncertainty regarding what could be the final say of the government on cross-border data transfer impacts businesses. They pointed out that this tentativeness impacts the expansionary policies of India, curtailing access to investments.

<sup>48</sup> Justice K.S. Puttaswamy (Retd) Vs Union of India (2017) 10 SCC 1.



### 3.2.3. OPERATIONAL CONCERN

In terms of operational impacts, start-ups noted that creating a separate system within the country where there is data localisation is concerning, especially if they are looking at commercially launching businesses. Some start-ups mentioned that while big companies may spend time and money on creating separate systems however that is not the case with smaller start-ups.

#### Key insights

- While some start-ups pointed out that there might be minimal macroeconomic repercussions, at the business level, they noted that the spending on homegrown technological infrastructure might get costlier for them.
- Some of the start-ups pointed out that the cost of data localisation is not always the economic cost, and it involves indirect costs which can't be quantified, like expertise and time.
- Start-ups pointed out that the price-sensitive Indian market would corner them to take on the additional compliance burdens and costs associated with the localisation mandate.
- Many start-ups pointed out that uncertainty regarding what could be the final say of the government on cross-border data transfer impacts businesses.
- Start-ups mentioned that while big companies may spend time and money on creating separate systems, that is not the case with smaller start-ups.

The DPDPB 2022 has relaxed the requirement for data localisation, i.e., to process and store data only in India. The draft permits the cross-border transfer of data with certain countries and territories that will be notified by the government based on the terms and conditions that it may specify.<sup>49</sup> In light of our extensive research and stakeholder engagement, as discussed above, removing data localisation to introduce trusted data flows to notified countries is a welcome move which would help the domestic start-up ecosystem to scale and overarchingly increase the quantum of digital trade.

However, as we move forward, it is critical for the government to establish a standardised procedure for determining the following– (a) countries to which data flow could happen, (b) a framework to be followed for data transfers and (c) mechanisms to be followed for data transfers.

---

<sup>43</sup> Clause 17, Digital Personal Data Protection Bill, 2022.

## 4. PRINCIPLE-BASED FRAMEWORK FOR DATA TRANSFERS

In addition to being a value proportion for certain classes of businesses, data goes far beyond becoming the core elements of a business model (refer to box 1) to provide smart services which use cutting-edge technologies like Artificial intelligence, augmented learning etc. For instance, the internal element which drives the Internet of Things, like smart home devices, is data.

### Box 1: Different types of Commercial Data Flows

1. **Transaction data flows between buyers and sellers at a market price, including direct purchases between buyers and sellers, such as in online banking or advertising, and services transactions that involve digital platforms acting as intermediaries between buyers and sellers.** These would include the invoice data that a marketplace platform collects when any transactions take place on their platform. The platform can use the data to manage inventory as well as optimise its algorithms to give more pointed recommendations to buyers.<sup>50</sup>
2. **Commercial data and services are exchanged between or within businesses or other related parties at a \$0 market price, including supply chain, personnel, or design information.** For instance, Scania and Volvo aggregate real-time data on vehicle positioning and diagnostics to improve safety, optimise supply chain management and assess and improve their cars' environmental impact. While these data points are not attributed to commercial value, they add to the company's ability to make better cars and even sell more of them as their brand image benefits from optimised service delivery.<sup>51</sup>
3. **Digital data and services delivered to and from end-users at a \$0 market price, including free email, search engine results, maps and directions, and information via social media.**<sup>52</sup> For instance, Google's Ad sense portal allows you to quantify your website's engagement and understand and get in touch with advertisers to increase revenue. In return, Google collects data from your website and the personal data that is shared by you. While the service is free, the data generated for and from the user generates value for both stakeholders.<sup>53</sup>

Quantifying the value of cross-border data flows and assessing their impact on economies becomes cumbersome as types 2 and 3 of the data flows mentioned above have no commercial values inherently but enable organisations to build systems that can generate value. Commercial data and services exchanged at the \$0 market often have associated revenues. For example, a firm might give away a "free service" to attract users to their site. Other firms pay to advertise their products or services on

<sup>50</sup> Marr, B. (2021 July 23) Amazon: Using Big Data to understand customers, Bernard Marr & Co. Retrieved on August 7, 2022 from <https://bernardmarr.com/amazon-using-big-data-to-understand-customers/>

<sup>51</sup> Casalini, F. & González J.L. (2019 January 23) *Trade and Cross-Border Data Flows*, OECD Organization for Economic Cooperation and Development (OECD) Trade Policy Papers, No. 220. Retrieved on June 21, 2022, from <https://dx.doi.org/10.1787/b2023a47-en>.

<sup>52</sup> Nicholson, J. & Noonan, R. (2014) *Digital Economy and Cross-Border Trade: The Value of Digitally-Deliverable Services*, Office of the Chief Economist, Economics and Statistics Administration (ESA), U.S. Department of Commerce. Retrieved on June 25, 2022, from <http://www.esa.doc.gov/sites/default/files/digitaleconomyandtrade2014-1-27final.pdf>

<sup>53</sup> Google AdSense, Blogpost: How AdSense works. Retrieved on August 7, 2022 from <https://support.google.com/adsense/answer/6242051?hl=en#:~:text=Google%20AdSense%20provides%20a%20way,want%20to%20promote%20their%20products.>

these sites, making it profitable for the first firm to offer free services to users. Services that are enabled through data flows allow for services to be provided for minimal or no costs and, in turn, add to the business. For instance, ‘freemium’ models allow users to use services for free, and access premium features for a fee added to the revenue that companies make. However, they do not have transactional values. These transactions are oftentimes not taken into consideration when data flows are studied to assess their impact on a country’s GDP.<sup>54</sup> The distinction between the three types mentioned above thus allows us to contextualise the various mechanisms of cross-border data flows that are expounded on below.

This development has transformed the goods and services trade which is increasingly digital and dependent on the free flow of data across borders. In addition, the internet is a network of networks which are interconnected and interdependent on various factors at the logical and application layer, where entity A would be dependent on entity B, who might be offshore. For instance, a fiduciary transfers, exchanges, ports and transmits data to a third party or other business units for various business purposes like processing, research and development, marketing, storage etc. Many businesses also pointed out restrictive data transfers can also hamper them from accessing innovative services which are available offshore. This shows that the seamless flow of data across the border is crucial for enabling innovation, economic proliferation, and competition at the international level, and data is becoming a yardstick for international trade and service delivery.

As India has relaxed data localisation to introduce trusted data flows to notified countries in its recent iteration of the data protection bill, as we move forward, it is important to establish a standardised framework to be followed for data transfers.<sup>55</sup> Therefore, through this chapter, we suggest that the Government of India must consider a principle-based framework as part of their engagement with other notified jurisdictions to enable free flow of data (through various means as discussed in chapter 5), which would later aid them in developing critical technology standards.

While domestic regulations of jurisdictions differ according to national priorities and objectives catering to sovereign goals, domestic constraints, etc. however, some principles like purpose limitation, transparency and accountability recognised by various domestic regulations are congruent (refer to chapter 2). Thus, the objective of the principle-based framework is to build consensus through balancing differences in national constraints and practices while respecting international principles to harmonise data regulation regimes for seamless implementation.<sup>56</sup> Besides, we expect the principle-based framework to create a trusted environment for countries to enable data transfers and minimise business compliance.

<sup>54</sup> Meltzer, J.P. (2020 July 28) *How APEC can address restrictions on cross-border data flows*, Australian Broadband Advisory Council (ABAC). Retrieved on June 23, 2022 from <https://app.glueup.com/resources/protected/organization/895/event/29824/f4ede14f-b70e-45a4-84e4-098bc975a67b.pdf>

<sup>55</sup> Shekar, K., & Rizvi, K. (2022, December 6). *Data Bill is a step forward in digital trade journey*. The Hindu Business Line. Retrieved December 16, 2022, from <https://www.thehindubusinessline.com/opinion/data-bill-is-a-step-forward-in-digital-trade-journey/article66231627.ece>

<sup>56</sup> Cory, N., Atkinson, R. D., & Castro, D. (2019, May 27). *Principles and Policies for “Data Free Flow With Trust”*. Information Technology and Innovation Foundation | ITIF. Retrieved July 26, 2022, from <https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust/>

There are various mechanisms through which cross-border data transfers happen for business-related data transfers, subject to the entity's nature. However, we propose a systematic way to approach cross-border data transfer mechanisms through this framework, where principles discussed in this chapter will be a prerequisite for various kinds of business-to-business data transfer chains, i.e., data fiduciaries to data fiduciaries, data fiduciaries to data processors and data fiduciaries to data storage facilities. For the purpose of this chapter, we discuss various principles across the data lifecycle bucketed and mapped to respective players within the data ecosystem.<sup>57</sup> While there are various players within the data ecosystem, for this chapter, we cover the four key players, i.e., data fiduciaries, intermediaries, data processors and data centres. In addition, this chapter also discusses principles for regulators/governments such that the implementation of a principle-based framework is seamless.

## 4.1. DATA FIDUCIARY DATA TRANSFERS

Data fiduciaries engage in cross-border data transfer, exchange, port and transmit data to a third party or other business units for various business purposes like processing, research and development, marketing, storage etc. In addition, they transfer data across border for data portability requests and to fulfil intra-group transfers, i.e., data transfers within the undertaking of businesses, franchises and branches, partners etc., which are located outside the country. Some jurisdictions provide data fiduciaries with various mechanisms to enable the free flow of data yet protect the privacy of individuals. Some of the critical mechanisms followed by jurisdictions at the individual level and consortium are:

**Adequacy decision:** This mechanism enables the free flow of data to other countries when the respective data protection authority is satisfied that the respective country where the data is intended to flow has adequate data protection. EU GDPR utilises this mechanism to enable data transfer outside the European borders ensuring domestic level data protection.<sup>58</sup>

As the fundamentals of data protection in the USA and Europe stand different, both countries signed a deal famously known as the US and EU Privacy Shield<sup>59</sup> to enable the free flow of data between the EU and USA corridor. However, recently Court of Justice of European Union (CJEU) struck down<sup>60</sup> the EU-US privacy shield arrangement like in the case of its predecessor, i.e., the safe harbour agreement.

CJEU struck down EU-US Privacy Shield as inadequate to protect the privacy and data of European Citizens. Some of the grounds under which this judgement was made are:

- While the US national security and law enforcement is essential, the court noted that it is interfering with European Citizens' fundamental right to privacy. This was revealed in whistleblower Edward Snowden's NSA revelation.<sup>61</sup>

<sup>57</sup> Stobierski, T. (2021, March 2). *5 Key Elements of a Data Ecosystem*. Harvard Business School Online. Retrieved June 23, 2022, from <https://online.hbs.edu/blog/post/data-ecosystem>

<sup>58</sup> Adequacy decisions. (n.d.). Retrieved from European Commission: [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)

<sup>59</sup> *Privacy Shield*. (n.d.). Retrieved December 19, 2022, from <https://www.privacyshield.gov/welcome>

<sup>60</sup> The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield. (2020). Retrieved from Court of Justice of the European Union: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf>

<sup>61</sup> MacAskill, E., MACASKILL, E., DANCE, G., CAGE, F., & CHEN, G. (2013, November 1). NSA files decoded: Edward Snowden's surveillance revelations explained. The Guardian. Retrieved January 13, 2022, from <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>

- In terms of judicial protection, the court pointed out that the ombudsperson mechanism in EU-US privacy, which helps mitigate the interference, is not up to the mark of EU laws.

These judgements have also brought concerns with the existing mechanism, which is not backed by a set of principles for various players (especially the government) involved in the cross-border data transfer pipeline. In addition, these judgements have also highlighted how differences in the domestic data protection landscape could create problems for mechanisms like adequacy decisions. However, the recent draft EU-US Data Privacy Framework follows some of the key principles discussed in this chapter, highlighting the importance of principle-level congruence.

However, similar to Europe, in Brazil, under the General Personal Data Protection Law (LGPD)<sup>62</sup>, Autoridade Nacional de Proteção de Dados (Brazil's data protection authority) determines the adequacy (it is referred to as Adequacy Determination<sup>63</sup>) of data protection at the recipient country or international organisation level to enable cross-border data transfer.

**Cross-Border Privacy Rules (CBPR):** While adequacy decisions at the jurisdiction level formally recognise other countries' data protection regulations to enable the free flow of data, at the business level, we have systems like CBPR. This is a government-provided data privacy certification for data fiduciaries to indulge in cross-border data transfers. The Asia-Pacific Economic Cooperation (APEC) first pioneered this mechanism by introducing a business-level privacy certification and country-level enforcement in case of violation.<sup>64</sup> Nine nations out of 21 APEC nations follow the CBPR system - the USA, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, Taiwan, and the Philippines.<sup>65</sup> The certified businesses can transfer data between APEC member economies (that have joined the CBPR system) using this system. Followed by this, the United States, Mexico and Canada committed to creating a unified cross-border data flow regime under the United States-Mexico-Canada Agreement<sup>66</sup>, recognising the CBPR system. Similarly, Japan amended its domestic data protection regulation recognising the CPBR system as a valid cross-border data transfer mechanism.<sup>67</sup>

**Market mechanisms:** Various market mechanisms allow data fiduciaries to prove their adequacy and help demonstrate compliance with data protection and privacy safeguards. Some of the prominent mechanisms are (a) **Certification schemes:** While CBPR is a government-provided certification, at the market level, data fiduciaries can also certify using government-recognised third-party data protection certification, which acts as a gate pass for cross-border data transfer. For instance, the Digital Economy Partnership Agreement (DEPA) between Singapore, Chile and New Zealand provisions for establishing data protection trustmarks/certificates as a valid mechanism to facilitate cross-border information transfers while protecting personal information.<sup>68</sup> (b) **Codes of conduct:** This mechanism allows trade associations and other representative bodies to formulate sector-specific guidelines and get them approved by the government. These guidelines are tailor-made to cater to data protection

<sup>62</sup> Brazilian General Data Protection Law (LGPD, English translation). (n.d.). International Association of Privacy Professionals. Retrieved January 16, 2022, from <https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/>

<sup>63</sup> Brazil: International data transfers | Insights. (n.d.). DataGuidance. Retrieved January 16, 2022, from <https://www.dataguidance.com/opinion/brazil-international-data-transfers>

<sup>64</sup> *What is the Cross-Border Privacy Rules System | APEC.* (n.d.). Asia-Pacific Economic Cooperation. Retrieved June 29, 2022, from <https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system>

<sup>65</sup> <http://cbprs.org/about-cbprs/>

<sup>66</sup> United States-Mexico-Canada Agreement | United States Trade Representative. (n.d.). USTR. Retrieved January 16, 2022, from <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement>

<sup>67</sup> Greenley, A. (2017, May 22). Japan's Amended Privacy Law to Go into Effect May 30, 2017 – CBPRs Recognized as an Approved Transfer Mechanism. TrustArc. Retrieved January 16, 2022, from <https://trustarc.com/blog/2017/05/22/japans-amended-privacy-law-go-effect-may-30-2017-cbprs-recognized-approved-transfer-mechanism/>

<sup>68</sup> *The Digital Economy Partnership Agreement (DEPA) - Singapore.* (n.d.). MTI. Retrieved June 29, 2022, from <https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement>

challenges shared by specific sectors or industries. Thus, these codes reflect the processes and functions of the data fiduciaries (within the industry) that had signed. The United Kingdom tests these mechanisms as part of its post-Brexit data transfer arrangements.<sup>69</sup>

**Binding Corporate Rules (BCR):** This mechanism provides adequate privacy safeguards for making restricted data transfers within the undertaking of data fiduciaries, franchises and branches, partners etc., which are located outside the country. This was developed and used as part of the EU GDPR, which remained unchanged in the UK GDPR post-Brexit.<sup>70</sup> Both countries ensure that data holders and data recipients sign BCR.

**Contractual Clauses:** While BCR is for restricted data transfers like intra-group data exchange, at the border level, data fiduciaries can use contractual clauses mechanisms with off-shore third-party organisations to transfer data. Using this, data fiduciaries can transfer data across borders by incorporating data protection clauses recognised by the government as part of the contract. For instance, the EU and UK have recognised or issued Standard Contractual Clauses.<sup>71,72</sup> Similarly, the Association of Southeast Asian Nations (ASEAN) has recognised model contractual clauses for data transfers.<sup>73</sup>

While these mechanisms take a principle-based approach, they are not holistic in nature, and many of these mechanisms hit a roadblock as they face friction with domestic regulations like in the case of the US-EU Privacy Shield discussed above. Therefore, as India moves toward enabling cross-border data transfers with other jurisdictions,<sup>74</sup> it is essential to consider a combination of the above-discussed mechanisms tailored to embed the principles discussed in the next section. During our engagement with start-ups and cloud service providers, about 84% of respondents expressed the need for a principle-based framework to enable cross-border data transfers and for ease of compliance.

The below-discussed principles would aid India and other jurisdictions in collaboratively determining data protection levels. The principles discussed below are mapped to exporters and importers, data processors, data centres, government and go-between players (refer to figure 1). For the purpose of this chapter, Data exporters are data fiduciaries with a domestic presence (any form) and follow respective domestic regulations. Data importers are offshore third parties (excluding processors and data centres) or the branch and franchise of the data exporters, business partners of the data exporter to whom the data is transferred for different purposes. The principles discussed in this chapter are the key universal and internationally recognised data protection and design principles embedded in various cross-border data transfer arrangements and data

<sup>69</sup> Swire, P. (2021, September 1). U.K.'s Post-Brexit Strategy on Cross-Border Data Flows. Lawfare Blog. Retrieved January 16, 2022, from <https://www.lawfareblog.com/uks-post-brexit-strategy-cross-border-data-flows>

<sup>70</sup> Binding Corporate Rules. (n.d.). ICO. Retrieved January 16, 2022, from <https://ico.org.uk/for-organisations/binding-corporate-rules/>

<sup>71</sup> Standard Contractual Clauses (SCC) | European Commission. (2021, June 4). European Commission. Retrieved January 16, 2022, from [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en)

<sup>72</sup> UK publishes own set of Standard Contractual Clauses. (2021, August 16). KPMG International. Retrieved January 16, 2022, from <https://home.kpmg/ch/en/blogs/home/posts/2021/08/uk-standard-contractual-clauses.html>

<sup>73</sup> ASEAN Model Contractual Clauses for Cross Border Data Flows. (n.d.). ASEAN.org. Retrieved January 16, 2022, from [https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows\\_Final.pdf](https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf)

<sup>74</sup> For instance, India indicated in the Comprehensive Economic Partnership Agreement with the United Arab Emirates the interest to promote electronic information flows across borders. Refer to: Comprehensive Economic Partnership Agreement (CEPA) between the Government of the Republic of India and the Government of the United Arab Emirates (UAE). (n.d.). Ministry of Commerce and Industry. Retrieved July 27, 2022, from <https://commerce.gov.in/wp-content/uploads/2022/03/Chapter-9.pdf>



protection regulations across jurisdictions<sup>75</sup>, including India.<sup>76</sup>

Some of the principles mapped to data exporters are extracted from GDPR, and India’s DPDPB 2022, like consent, individual rights of action, quality of data etc. The principles are also mapped from the explanatory note of the bill, which talks about 7 key principles of data protection.<sup>77</sup> Principles mapped to data importers are again advised by GDPR, and the cross-border transfer arrangements like CBPR, ASEAN Model Contractual Clauses for Cross Border Data Flows etc. Principles for data processors are advised by the US’s upcoming American Data Privacy and Protection Act, the World Economic forum’s data protection principles and APEC Privacy Recognition for Processors (PRP) system. Finally, principles for government/regulators are advised by The UN norms of responsible state behaviour in cyberspace.<sup>78</sup> Collectively, we believe the mapped principles (refer to figure 1) will enhance the digital trust of the individuals such that they feel at ease and safe sharing data and using the service.

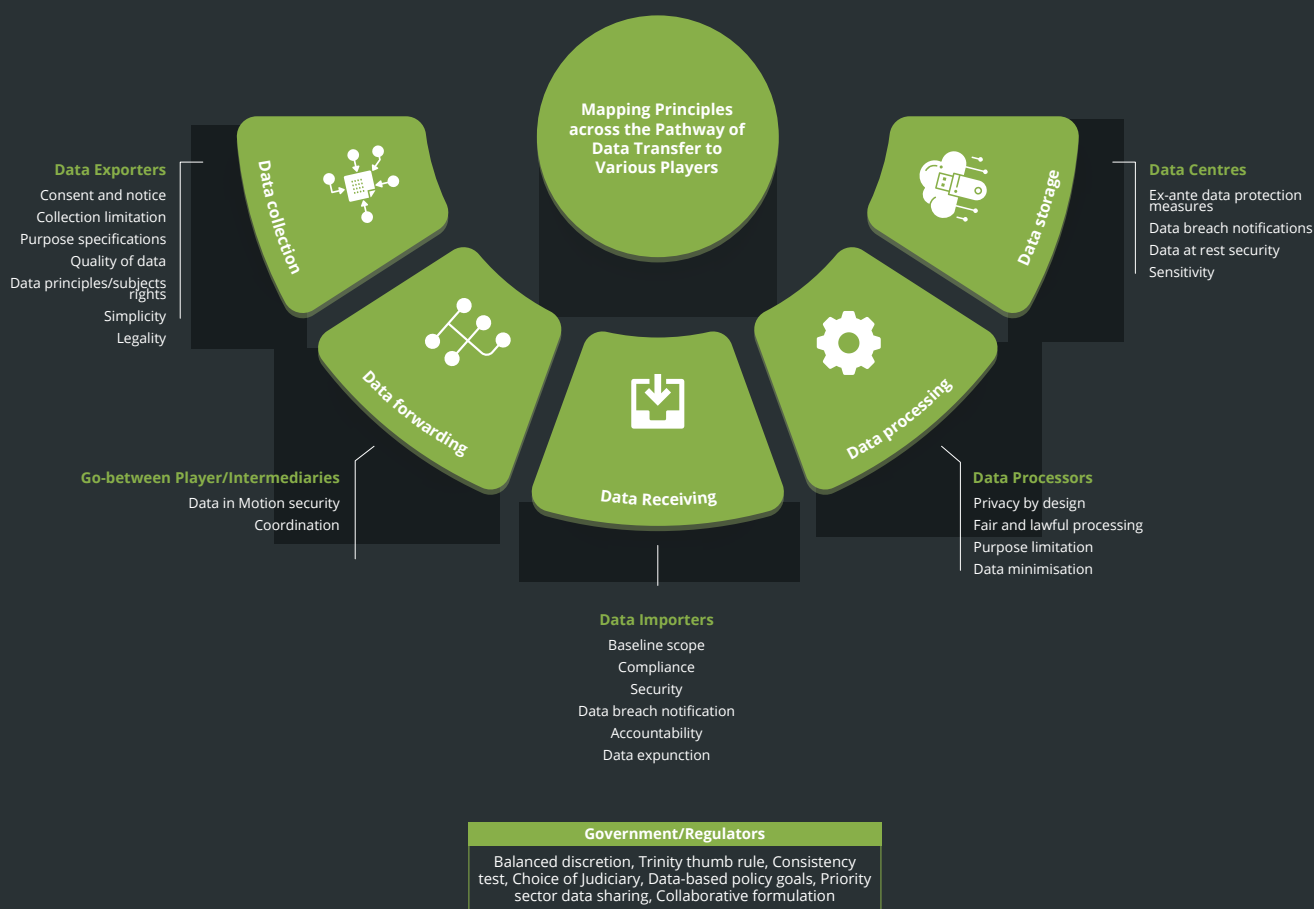


Figure 1

<sup>75</sup> For instance, The principles. (n.d.). ICO. Retrieved June 10, 2022, from <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/>; Healey, R. (2021, January 6). Malaysia Personal Data Protection Act 2010 - 7 Key Principles (Part 2). Lexology. Retrieved June 10, 2022, from <https://www.lexology.com/library/detail.aspx?g=e9444ef-e33e-4716-a920-17df5258267c>

<sup>76</sup> Sharma, D. (2020, May 22). Personal Data Protection Bill, 2019 –Examined through the Prism of Fundamental Right to Privacy – A Critical Study | SCC Blog. SCC Online. Retrieved June 10, 2022, from <https://www.sconline.com/blog/post/2020/05/22/personal-data-protection-bill-2019-examined-through-the-prism-of-fundamental-right-to-privacy-a-critical-study/>

<sup>77</sup> Explanatory Note - The Digital Personal Data Protection Bill, 2022. (n.d.). MeitY. Retrieved December 16, 2022, from <https://www.meity.gov.in/writereaddata/files/Explanatory%20Note-%20The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf>

<sup>78</sup> Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of. (2019, December 4). The United Nations. Retrieved July 27, 2022, from <https://www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf>



### 4.1.1. PRINCIPLES FOR DATA EXPORTERS

Data fiduciaries collect information about the consumers – directly through seeking information from the individuals and indirectly through third parties etc. However, the focus of business-related cross-border data transfers has been chiefly on data, i.e., directly collected from individuals. As it is futile to differentiate data based on transfers<sup>79</sup>, the principles discussed in this section are at the broader level of data collection done by data exporters with some specifics to cross-border data transfers.

**Consent and Notice:** The consumer must provide consent for the data collection and have adequate notice on how their data would be used and processed.<sup>80</sup> The adequate notice must also have clauses on cross-border data transfers such that data exporters don't have to seek permission separately every single time.

**Collection Limitation:** There shall be a limit to the extent of data collection via fair and appropriate means.<sup>81</sup> The data collected through inappropriate means must be barred from cross-border transfers. In addition, businesses must take reasonable steps to obtain the consent<sup>82</sup> of the individual for data collection, especially for cross-border data transfers.

**Purpose Specifications:** The purpose of data collection must be specified at the data collection stage. The data collected must be used only for the stipulated purpose, nothing incompatible with the specified purpose. Besides, in case of a change in purpose, the individuals must be notified for fresh consent. Also, the freedom to make changes to the purpose must be compatible with the original purposes.<sup>83</sup>

**Quality of Data:** The data collected must be cognate to the processing purpose, and such data must be accurate, complete and kept up-to-date. Businesses must take reasonable steps to minimise the harm caused by data inaccuracy due to incompleteness and lack of updates.

**Data Principles/Subjects Rights:** Rights like the right to data correction, right to be forgotten etc., must be vested in the hands of the individuals.<sup>84</sup> To exercise these rights, (a) businesses must constitute proper grievance redressal and various user-friendly mechanisms for the seamless exercise of individual rights and (b) must be associated with government-constituted active dispute resolution forums for particularly solving disputes related to cross-border data transfer.<sup>85</sup>

**Simplicity:** Consumer-facing privacy and data protection policies must be written in layman's terms. Those documents must enhance the ease of exercising informed consent by making policy simple to understand.

<sup>79</sup> Data Classification (Data Management): A Complete Overview. (n.d.). Spirion. Retrieved July 27, 2022, from <https://www.spirion.com/data-classification/>

<sup>80</sup> GDPR and CBPR follow the consent and notice principle. See here: GDPR matchup: *The APEC Privacy Framework and Cross-Border Privacy Rules*. (2017, May 31). International Association of Privacy Professionals. Retrieved June 21, 2022, from <https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/>

<sup>81</sup> Approved and recognised by various jurisdictions like the US, India, Europe etc.

<sup>82</sup> While we think consent-based mechanism has its cons, consent-based data collection is congruent to both India's upcoming data regulation and multiple data regulations outside India.

<sup>83</sup> *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. (n.d.). OECD. Retrieved June 21, 2022, from <https://www.oecd.org/digital/ieconomy/oecdguidelinesonthe-protection-of-privacy-and-transborder-flows-of-personal-data.htm>

<sup>84</sup> *A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy*. (n.d.). weforum.org. Retrieved June 21, 2022, from [https://www3.weforum.org/docs/WEF\\_A\\_Roadmap\\_for\\_Cross\\_Border\\_Data\\_Flows\\_2020.pdf](https://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf)

<sup>85</sup> Existing domestic dispute resolution mechanisms can be leveraged by constituting a separate wing or department for cross border data transfer disputes.

**Legality:** In concurrence with domestic regulations, grounds for collecting particular data from individuals must be legal depending on the sensitivity, criticality, cultural and religious value, sexuality etc.<sup>86</sup> In addition, businesses must comply with domestic regulations depending on the data type in terms of determining legality.

## 4.1.2. PRINCIPLES FOR DATA IMPORTERS

On receiving data from the data exporters, the data importers must ensure the data received is treated with at most protection as what it was treated in the home country. The data importers must have reasonable measures to ensure the data received is not misused. The reasonable measures must embed the principles listed below:

**Baseline Scope:** Data importers must process, use and store the data in accordance with the baseline scope (i.e., the scope of data processing) provided while entering the data transfer mechanism, i.e., contractual clauses, certification etc., which commends the data importers to follow principles like purpose limitation, accuracy, security safeguards, retention and accountability.<sup>87</sup>

**Compliance:** The compliance principle must be at two levels, i.e., (a) contract compliance in terms of complying with the contracts signed between data importers and data exporters in terms of usage, storing, and processing of the data transfers (b) regulatory compliance in terms of following domestic (to the importers) data protection the rules, regulations and practices for other compliances in addition to the principles discussed in this section for treating transferred data.

**Security:** Data importers must have technological and organisational structures and measures to maintain the integrity and confidentiality of the data received.<sup>88</sup> The measures must secure data from accidental loss, unauthorised processing, damage to integrity etc. The security principle must be scaled as per the risk associated with the sensitivity and quantity of the data received.

**Data Breach Notification:** Data importers must adopt a risk-based approach to report significant cyber incidents and data breaches as soon as practicable following a determination that it is a reportable incident. The data importers must consider reporting the incidents within 72 hours after detecting reportable breaches, which is a standard time followed by various jurisdictions.<sup>89</sup>

<sup>86</sup> For instance, in India caste data, is sensitive data that needs extra protection.

<sup>87</sup> ASEAN Model Contractual Clauses for Cross Border Data Flows. (n.d.). ASEAN. Retrieved June 22, 2022, from [https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows\\_Final.pdf](https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf)

<sup>88</sup> Art. 5 GDPR – Principles relating to processing of personal data - General Data Protection Regulation. (n.d.). GDPR. Retrieved June 22, 2022, from <https://gdpr-info.eu/art-5-gdpr/>; Principle (f): Integrity and confidentiality (security). (n.d.). ICO. Retrieved June 22, 2022, from <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/integrity-and-confidentiality-security/>

<sup>89</sup> Roth, J., & Alam, S. (2019, July 1). *Singapore Shakes Up Privacy: 72-Hour Breach Notice, New Guidance*. Lexology. Retrieved June 22, 2022, from <https://www.lexology.com/library/detail.aspx?g=b60894ce-79f2-4895-b4c3-3930fa97376f>; *Report of the Joint Committee on the Personal Data Protection Bill, 2019*. (2021, December 16). Retrieved June 22, 2022, from [http://164.100.47.193/Isscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17\\_Joint\\_Committee\\_on\\_the\\_Personal\\_Data\\_Protection\\_Bill\\_2019\\_1.pdf](http://164.100.47.193/Isscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf)

**Accountability:** Data importers must constitute an appropriate internal independent accountability mechanism like constituting a data handling officer and department (or assigned to other relevant existing departments) who would hold them accountable for complying with measures which give effect to the principles stated in this section.<sup>90</sup> Besides, this accountability structure must be funnelled to data exporters, where the data handling officer is contractually accountable to the respective department of data exporters.

**Data Expunction:** Data importers must adopt measures to delete the data post serving its purpose or in terms of termination of the contract with the data exporters.<sup>91</sup> They shall not retain received data beyond the period necessary to satisfy the purpose for which it is transferred. Also, the data must be deleted if data principals had sought the same through data exporters (through consent withdrawal) if they think it no longer serves the purpose.

## 4.2. PRINCIPLES FOR DATA PROCESSORS

Both data exporters and data importers process data for providing services to data principals, betterment of service delivery, marketing purpose, competition purpose etc. While processing of data by data exporters comes under the purview of domestic regulations of data exporters, the following principles, in addition to the principles discussed in Section 4.1.2, pertain to third parties data processors and cloud service providers that are stationed in other jurisdictions.

International practices provide various means and ways to enable cross-border data transfers between data fiduciaries and processors/cloud service providers. While enabling interoperability between data protection regimes would be a way forward, there are various market mechanisms like certifications which would aid data processors in proving their compliance with data protection regimes. For instance, APEC Privacy Recognition for Processors (PRP)<sup>92</sup> certifies data processors on data security practices and the ability to implement the relevant Cross-Border Privacy Rules (CBPR) requirements and other data privacy instructions of the data fiduciaries. As India<sup>93</sup> moves toward enabling cross-border data transfer for data processors, it must consider various mechanisms like PRP certification, accreditation etc., tailored to fit in the below discussed principles.

**Privacy by Design (PbD):** Data infrastructure and processing mechanism of data processors should be privacy-friendly and should not trade off privacy at the cost of business efficiency.<sup>94</sup> The concept of Privacy by Design (PbD) was first coined by Ann Cavoukian in the 1990s,<sup>95</sup> predating most data protection regulations.

<sup>90</sup> OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. (n.d.). OECD. Retrieved June 21, 2022, from <https://www.oecd.org/digital/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>; ASEAN Model Contractual Clauses for Cross Border Data Flows. (n.d.). ASEAN. Retrieved June 22, 2022, from [https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows\\_Final.pdf](https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf)<sup>92</sup> GDPR and CBPR follow the consent and notice principle. See here: GDPR matchup: *The APEC Privacy Framework and Cross-Border Privacy Rules*. (2017, May 31). International Association of Privacy Professionals. Retrieved June 21, 2022, from <https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/>

<sup>91</sup> Various jurisdictions including India, suggest data expunction through data protection regulations.

<sup>92</sup> *APEC Privacy Recognition for Processors ("PRP") Purpose and Background*. (n.d.). APEC CBPR. Retrieved May 3, 2022, from <https://cbprs.blob.core.windows.net/files/PRP%20-%20Purpose%20and%20Background.pdf>

<sup>93</sup> In the case of India - it provisions that data fiduciaries can't transfer data to data processors without a contract in place.

<sup>94</sup> Various data regulations in the world try to tackle this issue from the supply side by mandating Privacy by Design (PbD) as a design choice. PbD is a method through which privacy is embedded as part of technological developments and business processes. From a design-thinking perspective, PbD suggests that privacy must be approached at par with supply-side incentives such as innovations, competition, and creativity which are by default embedded within the technological systems and processes.

<sup>95</sup> Privacy by Design. (n.d.). Information and Privacy Commissioner of Ontario. Retrieved July 26, 2022, from <https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf>

PbD is a method through which privacy is embedded as part of technological developments and business processes. From a design-thinking perspective, Cavoukian suggests that privacy must be approached at par with supply-side incentives such as innovations, competition, and creativity which are by default embedded within the technological systems and processes. Therefore, data processors must follow seven foundational principles<sup>96</sup> extending beyond the below-discussed principles. Seven foundational principles are (a) Proactive, not reactive; preventative, not remedial<sup>97</sup>, (b) Privacy as the default<sup>98</sup>, (c) Privacy embedded into design<sup>99</sup>, (d) Full functionality – positive-sum, not zero-sum<sup>100</sup>, (e) End-to-end security – lifecycle protection<sup>101</sup>, (f) Visibility and transparency<sup>102</sup>, and (g) Respect for user privacy.<sup>103</sup>

**Fair and Lawful Processing:** Data processing must be consumer-centric. The results or actions of processing should not translate into exclusion and unfair discrimination<sup>104</sup> directly or as one of the unintended consequences.<sup>105</sup> Besides, processors must process data only when they have obtained it from legally authorised sources, given that the data is easily available in shadow markets and made available by unauthorised data brokers (in some cases unregulated).<sup>106</sup>

**Purpose Limitation:** Data processed by the data importer should not exceed the purpose that individuals consented to the data exporter (during data collection) and should not be held/stored post the completion of the purpose.

**Data Minimisation:** Data processed must be adequate and match the necessity of the purpose of such data so that it can be minimal, limited and confined to the purpose.

## 4.3. PRINCIPLES FOR DATA CENTRES

Data fiduciaries store data offshore in the cloud or on physical servers located across multiple geographies.<sup>107</sup> Data centres' biggest threat at the data storage stage is that of data breaches through hacking, leaks, etc. Data breaches cause reputational loss for data exporters and in addition, they also face heavy fines from domestic regulators and might get barred from engaging in cross-border data transfers. Thus, they have to exercise their oversight to ensure that the data centres which store the data offshore follow the below principles.

<sup>96</sup> Ibid.

<sup>97</sup> This principle talks about having robust ex-ante measures to preserve privacy than only having ex-post measures to remedy the violation.

<sup>98</sup> Privacy protection must be an automatic setting within technologies and business processes such that despite the lack of individual involvement, privacy is intact.

<sup>99</sup> Instead of having privacy as add-on settings, the processes and systems of technologies must have privacy as an integral component as part of core functionalities.

<sup>100</sup> Privacy should be a full functionality where technologies don't trade-off privacy at the cost of others.

<sup>101</sup> Privacy must be preserved throughout the lifecycle management of information where robust security measures are put in place to secure data, and necessary steps are taken to destroy the data at the end of the process securely.

<sup>102</sup> To ensure that technologies comply with the stated objectives, they must be subjected to independent verification to hold them accountable. Besides, their processes must be transparent to individuals, i.e., data subjects.

<sup>103</sup> Individuals, i.e., data subjects, must be kept at the topmost priority such that systems and processes of technologies offer firm privacy defaults, appropriate notice, and empowering user-friendly options.

<sup>104</sup> Radosavljevic, L. (2021, August 5). *The Key Principles of LGDP*. Helpy Pro. Retrieved June 23, 2022, from <https://helpy.io/blog/the-key-principles-of-lgdp/>

<sup>105</sup> *A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy*. (n.d.). weforum.org. Retrieved June 21, 2022, from [https://www3.weforum.org/docs/WEF\\_A\\_Roadmap\\_for\\_Cross\\_Border\\_Data\\_Flows\\_2020.pdf](https://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf)

<sup>106</sup> Raden, N. (2019, July 19). *Data brokers and the implications of data sharing - the good, bad and ugly*. Diginomica. Retrieved July 27, 2022, from <https://diginomica.com/data-brokers-and-implications-data-sharing-good-bad-and-ugly>

<sup>107</sup> Berry, I. (2021, September 20). *Top 10 Countries with the most data centres*. Data Centre Magazine. Retrieved July 27, 2022, from <https://datacentremagazine.com/top10-top-10-countries-most-data-centres>

**Ex-ante Data Protection Measures:** Data centres must have a robust set of ex-ante data protection measures (i.e., being proactive and constituting preventive mechanisms to secure data from harm) in place to ensure data imported for storing is prevented (rather than patched) from any harm.

**Data Breach Notifications:** Data centres must notify data exporters and designed government regulators about data breaches without undue delay (commonly followed is 72 hours from recognising the breach<sup>108</sup>). The data exporters must notify the individuals<sup>109</sup> and cease data transfers until the breach is fixed.

**Data at Rest Security:** Data centres must use various decentralisation of data storage mechanisms to reduce the risk of a data breach. Besides, data centres must show due diligence by using technologies for masking data at rest to weed out the reidentification threats.

## 4.4. PRINCIPLES FOR GO-BETWEEN PLAYER/ INTERMEDIARIES IN DATA TRANSFERS

Cross-border data transfer involves data exporters and data importers, data processors and data centres at the ends. However, as data gets forwarded to a third country, there are two key go-between players/intermediaries, connectivity providers and internet service providers etc. While most of the models and mechanisms are concerned with end players, through this principle-based framework, we take a holistic approach to cross-border data transfer where the below mentioned principles commend go-between players' compliance in addition to end players.

**Data in Motion Security:** Data in motion must be safeguarded from snooping, leak, manipulation, distraction etc., by having appropriate oversight (maybe by the data exporter) and accountability of go-between players.

**Coordination:** End players, i.e., data exporters and data importers, data processors, and data centres, must work in coordination with go-between players, especially with connectivity providers, such that any harm to the data while forwarding can be reported and prevented in the preliminary stage.

**Data Anonymity:** Data at motion must be anonymised in such a manner that the individual is no longer identifiable until the data reaches the destination, i.e., the data importer, processor, and data centres.

<sup>108</sup> Roth, J., & Alam, S. (2019, July 1). *Singapore Shakes Up Privacy: 72-Hour Breach Notice, New Guidance*. Lexology. Retrieved June 22, 2022, from <https://www.lexology.com/library/detail.aspx?g=b60894ce-79f2-4895-b4c3-3930fa97376f>; *Report of the Joint Committee on the Personal Data Protection Bill, 2019*. (2021, December 16). Retrieved June 22, 2022, from [http://164.100.47.193/lssccommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17\\_Joint\\_Committee\\_on\\_the\\_Personal\\_Data\\_Protection\\_Bill\\_2019\\_1.pdf](http://164.100.47.193/lssccommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf)

<sup>109</sup> In accordance with the domestic regulations.

## 4.5. PRINCIPLES FOR GOVERNMENT/REGULATORS

The zero steps towards implementing the principle-based framework would require domestic stability regarding data protection regulations. The primary regulatory issue would be recognising this framework as a legitimate lens to establish cross-border data transfers. If the data protection regulation and enforcement fall under the ambit of multiple regulators domestically, like in India (refer to box 2), recognition of this framework might not be uniform as some might recognise it while others refrain from it. In addition, the existence of different regulators/authorities will pave the way for multifarious interpretation/understanding of the framework, which gives birth to slightly different versions of the principle-based framework at the implementation level, causing confusion and conflict. Moreover, this conflict and differences at the implementation level will impact businesses, causing compliance uncertainty and regulatory arbitrage.<sup>110</sup> Also, businesses might find a way to comply only with the most favourable regulation, i.e., which allows cross-border data transfer at the cost of escaping other crucial mandates under other regulations. Therefore, consistent recognition and implementation of a principle-based framework for cross-border data transfer at domestic levels are crucial.

### Box 2: Case of Data Localisation

There could be various instances where sectoral regulations and guidance cross paths with some of the progressive measures to be established through DPDPB 2022. One of the key areas of contention would be with the measures taken at the level of localisation of data storage and processing. Although India's efforts to establish a data protection regime through DPDPB 2022 imply that data could flow across the border to notified countries under the bill, various other existing and upcoming sectoral regulations mandate the contrary, i.e., data localisation.

Some of the regulations which mandate data localisation are (a) Reserve Bank of India's 2018 circular titled "Storage of Payment System Data"<sup>111</sup>, which mandates conditional data localisation mandate, where end-to-end data relating to payment systems must be stored in India while it can be processed outside the territory of India, (b) Information Technology Act 2000 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 prohibits body corporates from transferring data across borders until the third party has adequate safeguards, (c) Amended Unified Access License agreement of Department of Telecommunications mandates telecom service providers to store and process subscribers information locally, (d) IRDAI (Outsourcing of activities by Indian Insurers) Regulation, 2017<sup>112</sup> mandates localisation of payholders' account details; in case of cross-border transfer the insurer must ensure easy regulatory access and oversight by the Authority. Besides, IRDAI (Maintenance of Insurance Records) Regulation, 2015<sup>113</sup> mandates organisations to store insurance data within the territory of India.

<sup>110</sup> Reducing the Risk of Policy Failure. (n.d.). OECD. Retrieved January 19, 2022, from <https://www.oecd.org/gov/regulatory-policy/1910833.pdf>

<sup>111</sup> Storage of Payment System Data. (2018). Retrieved from Reserve Bank of India: <https://www.rbi.org.in/scripts/NotificationUser.aspx?id=11244>

<sup>112</sup> Outsourcing of Activities by Indian Insurers Regulation, 2017. (2017). Retrieved from IRDAI: [https://www.irdai.gov.in/admincms/cms/frnGeneral\\_Layout.aspx?page=PageNo3149&flag=1](https://www.irdai.gov.in/admincms/cms/frnGeneral_Layout.aspx?page=PageNo3149&flag=1)

<sup>113</sup> Maintenance of Insurance Records Regulation, 2015. (2015). Retrieved from IRDAI: [https://www.irdai.gov.in/admincms/cms/frnGeneral\\_Layout.aspx?page=PageNo2604&flag=1](https://www.irdai.gov.in/admincms/cms/frnGeneral_Layout.aspx?page=PageNo2604&flag=1)

With these differences in regulations and guidance, it is technically impossible to process data by segregating it according to the difference in mandates. This would cause operational concerns for businesses, especially for the data processors and cloud service providers, as they must reprogram their systems. Also, aggregating data of individuals across the globe is essential for having better insights; however, when certain sets of data are restricted from flows across the border, this might hamper the businesses' data processing capabilities.

Therefore zero steps toward implementing trusted data flow would require domestic stability regarding data protection regulations. The primary regulatory issue would be recognising the importance of trusted data flows for enhancing the digital economy. If the data protection regulation and enforcement fall under the ambit of multiple regulators domestically, like in India, enabling the free flow of data like provisioned in DPDPB 2022 might not be uniform as some might recognise it while others refrain from it. Moreover, this conflict and differences at the implementation level will impact businesses, causing compliance uncertainty and regulatory arbitrage.

While enacting a new comprehensive data protection bill will bring overarching data protection regulation for India. However, concerns related to the harmonisation of various data regulations and coordination of various ministries and sectoral regulators remains unaddressed.

Though in the long term, it is ideal to have single consistent data protection regulation for India, in the short term, we would require high-level coordination amongst the regulators and policymakers to recognise and implement the principle-based framework for cross-border data transfers. There are provisions for coordination and harmonisation in some of the legislation and transfer framework and policy, including the previous versions of India's data protection bill (removed in new version), which could aid us in uniform recognition and implementation of the principle-based framework.

Therefore, the new bill must have provisions on Memorandum of Understanding (MoU) from the previous version (Clause 56 of PDP Bill 2019) where the proposed Data Protection Board (DPB) must enter a MoU with other regulators or authorities governing data to recognise the principle-based framework for cross-border data transfer. On the implementation front, MoU must recognise DPB as the central enforcement authority on cross-border data transfers. The DPB must be empowered to decide on at least one third-party accountability agency to verify the compliance of participating businesses with the principle-based framework. Besides, any dispute resolution related to cross-border data transfer must be addressed to DPB, which will coordinate with various coexisting grievance management systems and mandates under different regulations.



However, there are also various other roadblocks to implementing the principle-based framework for cross-border data transfer, which can't be solved exclusively at the domestic level. A concerted effort is needed between the signatory jurisdictions beyond its borders to enable data flow. Some of the key principles to be considered by the domestic regulators and governments in enhancing international-level coordination and cooperation are:

**Balanced Discretion:** While the principles allow for domestic-level discretion in implementation, this act has to be balanced where interpretation is not too different from the preamble of the principle-based framework, i.e., building consensus through balancing differences in national constraints and practices while respecting international principles. Besides, the exemption for securing national security and public order must be less discretionary. Concertedly, countries must lay down fair procedures and scenarios for exemptions.

**Trinity Thumb Rule<sup>114</sup>:** While jurisdictions have various economic and national interests to cater to, countries must strive to follow the trinity thumb rule, i.e., security, privacy and trade as part of any actions taken related to cross-border data transfer. These three elements also form the backbone of the principle-based framework for cross-border data transfers. Besides, countries must strive for a positive-sum game and not compromise on one element to achieve the other.

**Consistency Test:** Jurisdictions must refrain from enacting complicated and disparate future legislation or delegated regulations, which would hamper cross-border data transfers. Therefore, countries may recognise the principle-based framework as the foundation for cross-border data transfer, moving forward, countries must conduct a consistency test for any future legislation or regulations to check compatibility with the principle-based framework.

**Choice of Judiciary:** The critical concerns with bilateral agreements are that (a) courts should have jurisdiction over specific disputes, and (b) the system of law should govern specific issues. While it is futile to decide the choice of judiciary or jurisdiction as they may change according to the dispute, it is still essential to have guidelines for the same. Therefore, both signatory countries must work together to develop guidelines for the choice of judiciary and jurisdiction for various potential disputes to weed out uncertainty.

**Data-Based Policy Goals:** Some of the jurisdictions<sup>115</sup> (like discussed in Chapter 2) enact data localisation and restrict cross-border data transfers considering it has a mechanism to enhance security, privacy and access to data. However, the research/data points shows that either of these objectives can be substantially obtained through data localisation<sup>116</sup> and there are other optimal ways to obtain the same. Therefore, signatory jurisdictions must ensure that they adopt a data-based approach toward cross-border data transfer policy goal-setting so that they don't zero down on misguided goals. The jurisdictions must also closely monitor if some of the policy measures have any unintended restrictions on data transfers and cause splinternet.

<sup>114</sup> *Harmonising the UK and India Data Protection Regime*. (n.d.). The Dialogue | UKIBC. Retrieved July 27, 2022, from <https://thediologue.co/wp-content/uploads/2022/03/HARMONISING-THE-UK-AND-INDIA-DATA-PROTECTION-REGIME-The-Dialogue-UKIBC.pdf>

<sup>115</sup> Cory, N., & Dascoli, L. (2021, July 19). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. Information Technology and Innovation Foundation | ITIF. Retrieved June 23, 2022, from <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>

<sup>116</sup> *Ibid.*

<sup>117</sup> *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*. (n.d.). weforum.org. Retrieved June 30, 2022, from [https://www3.weforum.org/docs/WEF\\_Paths\\_Towards\\_Free\\_and\\_Trusted\\_Data%20Flows\\_2020.pdf](https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20Flows_2020.pdf)



**Collaborative Formulation:** Signatory Governments must actively engage with the private sector businesses<sup>117</sup> and other policy actors while defining some key terminology like personal data, non-personal data, metadata etc. Also, two signatory jurisdictions should work in tandem with respective businesses while defining sector-specific rules.

**Recognition of Accountability Principle:** The government and concerned regulators must acknowledge the different stakeholders in the data storage and processing chain, with varying responsibilities and control over personal data. Therefore, taking this into cognizance, government must recognise the internal independent accountability mechanism suggested in section 4.1.2, where data importers appoint a data handling officer who would be accountable to data exporters through contract.

The principles discussed in this section may be considered by India for enabling business-related cross-border data transfer mechanisms with other jurisdictions. Both India and other jurisdictions must aid businesses in implementing principles (irrespective of whichever mechanisms they choose) within their procedures and processes by forming various operational guidelines, Standard Operating Procedures, awareness programs, and private consultations. These aiding materials prepared by the governments must be tailored according to the domestic context and socio-economic-political fabric within which the businesses work for seamless implementation. Besides, moving forward, it is also crucial to identify one government agency as an enforcement authority<sup>118</sup> to supervise procedures and processes of businesses to see if they are aligned with the principles through mechanising various soft and hard enforcement measures. Also, the enforcement measures must be evaluated and implemented according to the nature and size of the non-compliance.

<sup>118</sup> For instance, in the case of India, it could be the DPB which would be formed post-enactment of the data protection bill.



# 5. IMPLEMENTATIONAL ROADMAP FOR A PRINCIPLE-BASED DATA TRANSFER FRAMEWORK

Coordination of various factors like regulatory landscape, geopolitics etc. is essential for the seamless implementation of the principle-based data transfer mechanism. This section explores the foundations for enhancing the digital economy partnership between India and other jurisdictions via adopting a principle-based data transfer framework as the government indicates the vision for trusted data flows to notified countries. While there are various means through which India can adopt a principle-based data transfer framework, in this chapter, we will discuss three key means, i.e., statutory mechanisms, bilateral agreements and multilateral arrangements.

## 5.1. STATUTORY MECHANISM

While the recent version of the Data Protection Bill allows trusted data flows to notified countries, there is less clarity in terms of mechanism for enabling such data transfers, like adequacy decisions in the case of Europe and the US. Therefore, to strengthen the ties with other jurisdictions in the future, as part of the new bill or subordinate regulations, India may consider a statutory mechanism to enable cross-border data transfers as mentioned below:

**Legislation:** As India is yet to establish a data protection regime and is currently drafting the same, it is ideal to have a principle-based data transfer framework with room for updating principles provisioned within it. A combination of the mechanisms discussed in chapter 4 must be provisioned within the bill or subordinate legislation such that it is tailored to embed the principles discussed. The statute must also provide clarity in terms of how the central government and data protection board can operationalise the same in tandem with their counterparts in other jurisdictions. Besides, the bill must also ensure that a principle-based data transfer mechanism is recognised consistently across sectoral regulations unless a legitimate state interest is hampered.

**Supervisory Authority:** During the trade negotiation, India must look for an independent supervisory authority in other jurisdictions (Like the FTC of the United States in case of business-related data transfers). However, India must make the DPB into a single point of contact and supervisory authority on matters related to cross-border data transfers mechanism. Besides, Sectoral or domain-specific regulators could work with the DPB to create regulations that consistently cross-reference each other, recognising principle-based data transfer framework. In addition, the legislation must ensure that DPB has considerable financial and functional independence and transparency in its operations with a robust accountability framework in place. DPB would need a steady and sustainable flow of revenue to keep its operations (a) seamless, (b) financially and functionally independent To achieve these goals, DPB must be allowed

through legislation to be funded through various facets. Besides, the legislation must provide DPB with the independence to decide on means and ways to generate revenue without hampering the functions with appropriate checks and balances to weed out moral hazards.

**International Commitment:** In dualist countries<sup>119</sup>, international laws and domestic laws are two different legal frameworks, where domestic laws precede and form the rule of the land. Here just the ratification of international obligations and principles is not enough, as the domestic laws must explicitly incorporate the same within the statute. In a welcome move, India is moving towards fulfilling its international commitments within its domestic legislation pertaining to data protection and privacy through clause 17 of the DPDPB 2022. At the same time, India must watch out for the same when it enters principle-based cross-border data transfers with other dualist countries. However, this would not be much of a concern in the case of a monist country like the United States (refer to Box 3).

**Rights Preserving Mandate:** As India enters a principle-based data transfer mechanism, it must ensure that the other jurisdictions have critical elements like democratic governance, civic and economic freedoms, human rights and equitable digital inclusion in the digital environment intact. (refer to chapter 6)

### Box 3: Dualist and Monist Countries

Most commonwealth countries are dualist states and follow various ways to incorporate treaties within the domestic legal systems. But in some dualist countries, signing a treaty is ineffective as they are not obliged to follow the same. Besides, antinomy in terms of contrast between domestic regulations and international commitments is noticed to be very high in these countries. However, this is not the case with the monist state.

In monist countries<sup>120</sup> international law becomes the rule of the land, with the state signing the international treaties as a commitment to the international principles and obligations, directly without incorporating it into the domestic legislation. Under this system, domestic legislation becomes subordinate; therefore, the ICC statute becomes enforceable within the national boundaries and adjudicated by the national courts. About 16 countries, like the US, Chile, Austria, South Africa etc., are monist states. In all 16 countries, in some form or other, it is mandated for the state to go for legislative approval before committing to international obligations for the nation.

<sup>119</sup> Self-executing treaties. (n.d.). Retrieved from The Peace and Justice Initiative: <http://www.peaceandjusticeinitiative.org/implementation-resources/dualist-and-monist/self-executing-treaties>; How does international law apply in a domestic legal system? (n.d.). Retrieved from The Peace and Justice Initiative: <https://www.peaceandjusticeinitiative.org/implementationresources/dualist-and-monist>

<sup>120</sup> Ibid.

## 5.2. TRADE ARRANGEMENTS

In a globalised world, the internet and technological developments have transformed the goods and services trade which is increasingly digital and dependent on the free flow of data across borders. As data is becoming a yardstick for international trade, through this section, we will explore the foundation for adopting principle-based data transfer as a means to have solid data and digital trade partnerships between India and other jurisdictions.

### 5.2.1. MULTILATERAL ARRANGEMENTS

There are various existing multilateral frameworks (both binding and non-binding) that India could utilise to introduce principle-based data transfer mechanisms. The arrangements discussed in this section include agreements, strategies, and declarations to which India is currently a signatory, as well as arrangements to which India could potentially consider being a signatory in future for enabling the free flow of data.

**Indo-Pacific Strategy:** This strategy<sup>121</sup> proposes an Indo-Pacific economic framework to govern the digital economies, and cross-border data flows according to open principles. While India opted out of the “trade” pillar of the Indo-Pacific Economic Framework (IPEF)<sup>122</sup>, it was done at a time when India’s domestic draft data protection bill restricted cross-border data transfer. With the new draft bill permitting data transfer to notified countries, India’s domestic stance indicates a progressive steps towards data flows. Therefore, with a relaxed position on data transfers in the upcoming DPDPB 2022, we suggest India could consider joining the “trade” pillar of the IPEF and open a pact to enable data transfer with the United States by introducing the principle-based data transfer mechanism.<sup>123</sup> The Indo-Pacific strategy also intends to work with APEC on trade. This statement does show the United States’ potential interest in the APEC’s Cross-border Privacy Rules (CBPR) System for cross-border data transfers. With the CBPR system being made available to countries beyond APEC<sup>124</sup>, again India can consider opening a potential conversation on the principle-based data transfers mechanism to the CBPR cohort as well.

**QUAD:** The QUAD nations must move forward with establishing an FTA separately that lays the ground for cross-border data transfers by adopting a principle-based framework. While FTAs between Australia and India are in the works<sup>125</sup> and are expected to increase trade across industries. There is still no talk of data transfers between India and other QUAD nations. Therefore leveraging this opportunity, India must introduce principle-based cross-border data transfers with QUAD nations.

<sup>121</sup> *INDO-PACIFIC STRATEGY*. (n.d.). The White House. Retrieved June 5, 2022, from <https://www.whitehouse.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf>

<sup>122</sup> *On India opting out of IPEF: India must actively pursue trade agreements, not only bilateral ones but also plurilateral pacts*. (2022, September 14). The Indian Express. Retrieved October 21, 2022, from <https://indianexpress.com/article/opinion/editorials/on-india-opting-out-of-ipef-india-must-actively-pursue-trade-agreements-not-only-bilateral-ones-but-also-plurilateral-pacts-8149340/>

<sup>123</sup> Shekar, K. (2022, September 30). *Exploring a roadmap for digital trade*. Times of India. Retrieved October 21, 2022, from <https://timesofindia.indiatimes.com/blogs/voices/exploring-a-roadmap-for-digital-trade/>

<sup>124</sup> Kurth’s, A., & Kurth, A. (2022, April 21). *Global APEC Cross-Border Privacy Rules*. National Law Review. Retrieved June 5, 2022, from <https://www.natlawreview.com/article/apec-cross-border-privacy-rules-go-global>

<sup>125</sup> Dan Tehan (2021 October 1st) *Australia - India trade Deal*, Trade Minister, Australia, accessible from <https://www.trademinister.gov.au/minister/dan-tehan/media-release/australia-and-india-trade-deal>

**Joint Declaration on Privacy and the Protection of Personal Data<sup>126</sup>:** To strengthen trust in the digital environment, India signed a declaration with the European Union, Australia, Comoros, Japan, Mauritius, New Zealand, the Republic of Korea, Singapore, and Sri Lanka. The declaration tries to foster international cooperation to promote high data protection and privacy standards shared across the Indo-Pacific region, Europe and beyond. This is a step in the right direction as the declaration tries to promote a principle-based framework to enhance trust. Therefore, as this declaration aims to establish a trusted digital environment, India must try to push for a principle-based data transfer mechanism with the signatories and to get more support for this declaration.

**Data Free Flow with Trust:** While data increasingly drives the digital trade and economy. Yet, we see divergence and inconsistency in domestic data governance policies and regulations. Against this backdrop, at the 2019 G20 Osaka Summit, Japan proposed international coordination in terms of enabling cross-border data transfers by building consensus on domestic regulations under the Data Free Flow with Trust (DFFT) vision.<sup>127</sup> At the summit, 78 like-minded WTO members signed the “Osaka Declaration on Digital Economy”<sup>128</sup> to launch the Osaka track to demonstrate their commitment to promoting efforts in international rule-making on the digital economy. However, India refrained from Data Free Flow with Trust<sup>129</sup> for one of the reasons being an absence of data protection regulations domestically. However, the recent G20 Leaders’ Declaration<sup>130</sup> and domestic developments with DPDPB 2022 show that things have evolved since 2019. Besides, India also considered DFFT to be not comprehensive enough to incorporate aspects of various data protection legislation across the globe. Therefore, as Japan will be hosting the G7 summit in 2023 and expressed interest in upgrading the DFFT<sup>131</sup>, India must utilise this window to move the forward on a principle-based data transfer approach within the DFFT vision, which is more balanced and pragmatic.

**G20 Leader’s Riyadh Declaration:** During the Riyadh summit, G20 leaders stood united on multilateral cooperation in tackling some of the key concerns of the 21st century through the Riyadh declaration to extract the opportunities.<sup>132</sup> One of the key areas discussed in the declaration was the digital economy, under which they acknowledged the importance of data-free flow with trust and cross-border data flows. In addition, they also reaffirmed the role of data in development. Expanding on these commitments, as India will be hosting the G20 summit in 2023<sup>133</sup>, it could use this window to push for a principle-based data transfer framework for the free flow of data amongst the G20 nations. We could champion data free flow with trust to arrive at principles for protecting user data, privacy and data security as part of a broader multilateral arrangement amongst the G20 nations, which could subsequently facilitate digital trade in the future.

<sup>126</sup> *Joint Declaration by India, the European Union, Australia, Comoros, Japan, Mauritius, New Zealand, the Republic of Korea, Singapore, Sri Lanka on privacy and the protection of personal data: Strengthening trust in the digital environment.* (2022, March 21). Ministry of External Affairs. Retrieved June 5, 2022, from <https://mea.gov.in/bilateral-documents.htm?dti/35001/Joint+Declaration+on+privacy+and+the+protection+of+personal+data+Strengthening+trust+in+the+digital+environment>

<sup>127</sup> *Osaka Declaration on Digital Economy.* (n.d.). G20 2019 Japan. Retrieved June 30, 2022, from [https://www.mofa.go.jp/policy/economy/g20\\_summit/osaka19/pdf/special\\_event/en/special\\_event\\_01.pdf](https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/special_event/en/special_event_01.pdf)

<sup>128</sup> *Ibid*

<sup>129</sup> Mishra, A. R. (2020, September 22). *India says no to free flow of digital data at G20 meeting.* Mint. Retrieved June 30, 2022, from <https://www.livemint.com/news/india/india-says-no-to-free-flow-of-digital-data-at-g20-meeting-11600787726265.html>

<sup>130</sup> G20 BALI LEADERS’ DECLARATION Bali, Indonesia, 15-16 November 2022. (2022, November 16). Retrieved December 12, 2022, from <https://web.kominfo.go.id/sites/default/files/G20%20Bali%20Leaders%27%20Declaration%2C%2015-16%20November%202022%2C%20incl%20Annex.pdf>

<sup>131</sup> *Data Free Flow with Trust, now entering implementation phase.* (2022, May 20). The World Economic Forum. Retrieved June 30, 2022, from <https://www.weforum.org/agenda/2022/05/cross-border-data-regulation-dfft/>

<sup>132</sup> *Leaders’ Declaration.* (2020, November 22). G20 Riyadh Summit. Retrieved June 30, 2022, from [http://www.g20.utoronto.ca/2020/G20\\_Riyadh\\_Summit\\_Leaders\\_Declaration\\_EN.pdf](http://www.g20.utoronto.ca/2020/G20_Riyadh_Summit_Leaders_Declaration_EN.pdf)

<sup>133</sup> Chaudhury, D. R. (2020, November 23). *India to host G20 Summit in 2023; Riyadh summit eyes to spur growth & control virus.* The Economic Times. Retrieved June 30, 2022, from <https://economictimes.indiatimes.com/news/politics-and-nation/india-to-host-g20-summit-in-2023-riyadh-summit-eyes-to-spur-growth-control-virus/article-show/79360599.cms>

## 5.2.2. BILATERAL ARRANGEMENTS

There are various existing and upcoming bilateral arrangements between India and other jurisdictions. This section will discuss the strategy of using the existing/upcoming arrangements to establish and enable principle-based data transfers. While enabling cross-border data transfers is overwhelmingly beneficial, it is more lucrative to enable the same with countries which share a positive relationship in trade, investments etc. Therefore, though there are various bilateral arrangements, in this section, we will be discussing some of the key bilateral arrangements with key jurisdictions like the EU<sup>134</sup>, US<sup>135</sup>, Australia<sup>136</sup>, UK<sup>137</sup>, UAE<sup>138</sup>, Japan<sup>139</sup>, and Singapore.<sup>140</sup>

**Indo-EU Arrangement:** After 8 years, EU-India resumed the talks for a balanced and comprehensive trade pact and concluded the first round of negotiations on 2nd July 2022.<sup>141</sup> During the EU-India FTA Negotiations, the EU submitted a draft proposal for a legal text on Digital Trade. The draft is currently tabled for further discussions and will only be finalised after the negotiation rounds. Therefore, as India opens up for the free flow of data to trusted geographies with DPDPB 2022 to be enacted sooner, this presents the opportunity to India to boost trade relations with the EU and avoid new and unnecessary technical barriers through adopting principle-based data transfers framework.

**Indo-US Bilateral Arrangement:** India has about 50 Bilateral Trade Agreements with the United States over technology, military and other industry knowledge sharing and commodity trading. However, none of the trade agreements has provisions for data transfers. Therefore, these trade agreements must be tweaked to safeguard our data interests as well as facilitate the free flow of data between the two countries.<sup>142</sup>

One of the key trade agreements which India and the US can leverage for establishing principle-based data transfers is *India - US Science and Technology Cooperation Agreement (SCT 2019)*.<sup>143</sup> The SCT 2019 between the two countries has relatively more intensive Intellectual Property protection as well as an acceptance of data as a valuable asset being transferred between the two countries. Article VIII of the agreement covers all scientific data transfers between the two nations. However, it doesn't have a commercial element but rather a scientific knowledge exchange. Thus, it is of prime importance that the principle-based data transfer mechanism is negotiated through this agreement to initiate a commercial element, i.e., business-related data transfers between two countries.

<sup>134</sup> Laskar, R. H. (2022, July 18). India-EU FTA talks to focus on digital trade, data security, sustainability: Sources. Hindustan Times. Retrieved December 21, 2022, from <https://www.hindustantimes.com/india-news/indiaeu-fta-talks-to-focus-on-digital-trade-data-security-sustainability-sources-101658153156590.html>

<sup>135</sup> *The Future of Expanding India-USA Bilateral Relations: Strengthening bilateral ties through FTA 1* | PHD Research Bureau. (n.d.). PHD Chamber. Retrieved May 20, 2022, from <https://www.phdcci.in/wp-content/uploads/2020/11/The-Future-of-Expanding-India-USA-Bilateral-Relations-Strengthening-bilateral-ties-through-FTA.pdf>

<sup>136</sup> India, Australia should look at \$100 bn bilateral trade by 2030: Goyals. (2022, April 6). Business Standard. Retrieved June 16, 2022, from [https://www.business-standard.com/article/economy-policy/india-australia-should-look-at-100-bn-bilateral-trade-by-2030-goyal-122040600233\\_1.html](https://www.business-standard.com/article/economy-policy/india-australia-should-look-at-100-bn-bilateral-trade-by-2030-goyal-122040600233_1.html)

<sup>137</sup> International data transfers: building trust, delivering growth and firing up innovation. (2021, August 26). GOV.UK. Retrieved March 21, 2022, from <https://www.gov.uk/government/publications/uk-approach-to-international-datatransfers/international-data-transfers-building-trust-delivering-growth-and-firing-up-innovation>

<sup>138</sup> Sirohi, S. (2022, April 21). *Historic India-UAE trade pact effective from May 1: Minister*. The Economic Times. Retrieved July 1, 2022, from <https://economictimes.indiatimes.com/news/economy/foreign-trade/historic-india-uae-trade-pact-effective-from-may-1-minister/articleshow/90974901.cms>

<sup>139</sup> CHAUDHURY, D. R. (2021, October 13). *Indo-Japan trade increases to \$ 18 bn in 2019: Exim Bank study*. The Economic Times. Retrieved July 1, 2022, from <https://economictimes.indiatimes.com/news/economy/foreign-trade/indo-japan-trade-increases-to-18-bn-in-2019-exim-bank-study/articleshow/86983132.cms>

<sup>140</sup> Sirohi, S. (2021, May 28). *India-Singapore trade likely to be around \$21 billion in 2020-21*. The Economic Times. Retrieved July 1, 2022, from <https://economictimes.indiatimes.com/news/economy/foreign-trade/india-singapore-trade-likely-to-be-around-21-billion-in-2020-21/articleshow/83030231.cms>

<sup>141</sup> India-EU conclude 1st round of negotiations for India-EU Trade and Investment Agreements; 2nd round of negotiations scheduled to take place in September 2022 at Brussels. Retrieved December 21, 2022, from <https://pib.gov.in/PressReleaseSelfFramePage.aspx?PRID=1838839>

<sup>142</sup> *India-US Bilateral Relations Overview: Shared democratic values and growing convergence on bilateral, regional, and global i*. (n.d.). Embassy of India, Washington DC, USA. Retrieved June 5, 2022, from <https://www.indianembassyusa.gov.in/pdf/menu/IndiaUSNew2021.pdf>

<sup>143</sup> *AGREEMENT ON SCIENTIFIC AND TECHNICAL COOPERATION WITH INDIA*. (n.d.). State Department. Retrieved June 5, 2022, from <https://www.state.gov/wp-content/uploads/2020/04/19-1216-India-Scientific-and-Technical-Cooperation-India-09.20.2019-09.23.2019.pdf>



**Indo-Australia Bilateral Arrangement:** During the 17th joint Ministerial Commission, India and Australia relaunched the Australia-India Comprehensive Economic Cooperation Agreement<sup>144</sup> negotiations and committed to concluding a bilateral agreement between the two jurisdictions by the end of 2022. With the elevation of the Australia-India relationship to a Comprehensive Strategic Partnership (CSP)<sup>145</sup> which includes a commitment to encourage expanded trade and investment flow to the benefit of both economies, the nature of the data governance regime will have a significant impact on existing and potential Australian trade with India. As both countries are keen on signing a digital trade agreement,<sup>146</sup> it would be an ideal window for them to negotiate on incorporating the principle-based data transfers framework. This negotiation should ensure the free flow of data between India and Australia across borders using various mechanisms bedrock on the principle-based framework discussed in chapter 4.

**Indo-UK Bilateral Arrangement:** India and the United Kingdom have recently concluded five rounds of the India-UK Free Trade Agreement (FTA)<sup>147</sup>. While there are some delays in signing the India-UK FTA,<sup>148</sup> however negotiations still present both governments with an opportunity to create a data transfer framework that can enable seamless data flow to facilitate economic growth and innovation in both countries. Digital trade through goods and services has been one of the key areas negotiated. To maximise the benefits and achieve the full potential of the India-UK digital trading relationship, both countries must negotiate adopting a principle-based data transfer framework to have a seamless flow of data between the two countries. While initially data sharing was skipped as part of the India-UK FTA negotiations, due to a lack of data protection and e-commerce regulation<sup>149</sup>, in our recent study<sup>150</sup>, we highlight the potential roadblocks to a data transfer agreement between India and UK and lay out the means to mitigate the same. Also, relaxing data localisation to introduce trusted data flows within the Digital Personal Data Protection Bill 2022 would aid India in exploring the foundation for a solid digital trade partnership through consensus building and trust with the UK.

**Indo-UAE Bilateral Arrangement:** India recently signed a Federal Trade Agreement (FTA) with the United Arab Emirates marking the first Indian FTA that had a section on the Cross-Border Flow of information within the digital economy chapter.<sup>151</sup> Under the section on the cross-border flow of information, both countries recognise the importance of the flow of information for facilitating trade while protecting personal data. Moreover, India and UAE are also committed to promoting electronic information flow across borders subject to the legal and regulatory frameworks. In continuation of this commitment, India must foster ties with the UAE by introducing a principle-based data transfer framework at the implementation level to enable the free data flow between the UAE and India.

<sup>144</sup> Australia-India Comprehensive Economic Cooperation Agreement (AI-CECA). (n.d.). Department of Foreign Affairs and Trade. Retrieved July 1, 2022, from <https://www.dfat.gov.au/trade/agreements/negotiations/aifta/australia-india-comprehensive-economic-cooperation-agreement>

<sup>145</sup> Joint Statement on a Comprehensive Strategic Partnership between Republic of India and Australia. (n.d.). Department of Foreign Affairs and Trade. Retrieved July 1, 2022, from <https://www.dfat.gov.au/geo/india/joint-statement-comprehensive-strategic-partnership-between-republic-india-and-australia>

<sup>146</sup> Australia hopes digital trade agreement with India by the year-ends. (2022, April 27). Business Standard. Retrieved July 1, 2022, from [https://www.business-standard.com/article/economy-policy/australia-hopes-digital-trade-agreement-with-india-by-the-year-end-122042700036\\_1.htm](https://www.business-standard.com/article/economy-policy/australia-hopes-digital-trade-agreement-with-india-by-the-year-end-122042700036_1.htm)

<sup>147</sup> India and UK conclude fifth round of talks for India-UK Free Trade Agreement. (2022, August 11). PIB. Retrieved August 20, 2022, from <https://pib.gov.in/PressReleasePage.aspx?PRID=1850835>

<sup>148</sup> Laskar, R. H. (2022, October 20). India, UK unlikely to finalise Free Trade Agreement before 2023. Hindustan Times. Retrieved October 21, 2022, from <https://www.hindustantimes.com/india-news/india-uk-unlikely-to-finalise-free-trade-agreement-before-2023-101666290040740.html>

<sup>149</sup> Mishra, R. D. (2022, April 6). Data sharing may be a no-go area for now under UK FTA. Mint. Retrieved July 1, 2022, from <https://www.livemint.com/technology/tech-news/data-sharing-may-be-a-no-go-area-for-now-under-uk-fta-11649185425183.html>

<sup>150</sup> Shekar, K., Tripathi, A., Venkatesh, K., & Misra, M. (n.d.). Harmonising The UK AND India Data Protection Regime. The Dialogue | UK IBC. Retrieved July 1, 2022, from <https://thediologue.co/wp-content/uploads/2022/03/HARMONISING-THE-UK-AND-INDIA-DATA-PROTECTION-REGIME-The-Dialogue-UKIBC.pdf>

<sup>151</sup> Chapter 9 - Digital Trade. (n.d.). Ministry of Commerce and Industry. Retrieved July 1, 2022, from <https://commerce.gov.in/wp-content/uploads/2022/03/Chapter-9.pdf>



**Indo-Japan Bilateral Arrangement:** In 2011, India signed a Comprehensive Economic Partnership Agreement with Japan,<sup>152</sup> however, the agreement doesn't have any indication or commitment related to digital trade. The landscape has changed since 2011, with technological developments transforming the goods and services trade which is increasingly digital and dependent on the free flow of data across borders. Therefore, to achieve two of the key objectives of the Indo-Japan CEPA, i.e., (a) to liberalise and facilitate trade and (b) to improve the business environment, India must consider reviewing the agreement under Article 71. As part of the review, India could push for a principle-based cross-border data transfer framework to enable the free data flow between India and Japan.

**Indo-Singapore Arrangement:** In 2005, India entered a Comprehensive Economic Cooperation Agreement with Singapore. While the agreement has a chapter on E-Commerce<sup>153</sup>, it does not have much detail on the importance of and commitment to cross-border data transfers for enhancing the trade and business environment. However, as discussed earlier in the case of Japan, technology has changed the paradigm of trade which is currently heavily dependent on data flows. Therefore, India must consider refreshing the ties with Singapore on the base of the existing CEPA to keep up with time and negotiate for a principle-based data transfer framework for the free flow of data across borders.

Similar to the above-discussed bilateral arrangements with key jurisdictions, India has ongoing and settled trade agreements with countries like Korea, Malaysia, Canada, Mauritius, Africa, Brazil etc. As some of these agreements are dated, it is ideal for India to rekindle conversation on catching up with time with other jurisdictions to incorporate aspects related to digital trade, especially the principle-based cross-data transfer framework. Besides, as India is still in the negotiation stage with countries like Canada, it should use this opportunity to negotiate for incorporating a principle-based data transfer framework.

<sup>152</sup> *Comprehensive Economic Partnership Agreement Between Republic of Indian and Japan*. (n.d.). Department of Telecommunications. Retrieved July 1, 2022, from <https://dot.gov.in/sites/default/files/India%20Japan%20CEPA%2016.02.2011.pdf>

<sup>153</sup> *CHAPTER 10 - E-Commerce*. (n.d.). Ministry of Commerce. Retrieved July 1, 2022, from <https://commerce.gov.in/wp-content/uploads/2020/05/ch10.pdf>



## 6. PRIORITY AREAS FOR GOVERNMENTAL NEGOTIATION

A principle-based framework is the need of the hour to ensure a smooth flow of data across borders, and it is essential to operationalising the same using some of the key mechanisms discussed in chapter 5. However, it is important for the Indian government to consider some of the key parameters discussed in this chapter to be satisfied by the other jurisdictions for enabling such transfers through principle-based data transfer agreements.

The notion of sovereignty on which data localisation is based must be revisited, considering the borderless nature and openness of the digital space in which data flows. In digital space, the sovereignty of data must be balanced with the individual and community data rights, and they should be given more control over their data to prevent misuse. Having said that, cross-border data flow should be governed by a broader framework which keeps the interest of the data principals and businesses on an equal pedestal. It would help in the free flow of data across borders under a set of regulations and will not have to conform to the changing norms in every country. In the interviews, stakeholders highlighted that a global framework or at least a principle-based framework at a global level would immensely help businesses transfer data to recipient countries. Isolationist or protectionist measures may be avoided as they are not likely to pay because of the character of the internet and the interdependence of the data-driven digital economy. This is where negotiations with other countries in terms of data protection measures come into place.<sup>154</sup>

The growth of the data value chain offers opportunities for developing countries to build capacities, but it is important to emphasise that most data and data collection infrastructure are privately driven and controlled by large firms that are predominantly not located in developing countries, with the notable exception of China. There are, therefore, significant capacity challenges at an individual, firm and policy level to ensure that developing countries are not just sites of data collection, but that they can capture value from data.<sup>155</sup> Besides, industry representatives expressed that to extract value from data, it is essential to have access to a mix of inland and offshore innovative services for which cross-border data transfer is essential.

A lack of consistent approaches to regulating cross-border data flows will likely lead to suboptimal outcomes. As discussed earlier, the assessments of the value of data vary from one stakeholder to the other, with further complexities in the international sphere. The developing world, for instance, may not always have a data protection regulation conducive to supporting smooth international data flows.<sup>156</sup> This extends beyond the legislative framework to include the infrastructure and capabilities of relevant actors. Fostering a data exchange system through a global framework which can be adhered to by the majority of countries would allow for more inclusive and sustainable outcomes.<sup>157</sup> A reference can be taken from the Inclusive Framework

<sup>154</sup> Gibson, M., & Quiros, D. (2021, September 29). *Digital Economy Report 2021*. UNCTAD. Retrieved August 22, 2022, from [https://unctad.org/system/files/official-document/der2021\\_en.pdf](https://unctad.org/system/files/official-document/der2021_en.pdf)

<sup>155</sup> Ibid.

<sup>156</sup> Ibid.

<sup>157</sup> World Economic Forum, "A Roadmap for Cross - Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy" White Paper World Economic Forum (June 2020) Available At: [https://www3.weforum.org/docs/WEF\\_A\\_Roadmap\\_for\\_Cross\\_Border\\_Data\\_Flows\\_2020.pdf](https://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf)

for cross-border taxation of companies developed by OECD, which has been agreed upon by 136 countries.<sup>158</sup> A similar approach can be taken with the cross-border data flow, where a multilateral framework can be developed.

Keeping in mind the principles mentioned in chapter 4, there are certain key areas and standards which are of utmost importance and have to be looked into. The report identifies four such key areas which have to be deliberated upon while entering into any bilateral or multilateral framework as they form the bedrock for enabling the smooth flow of data. For instance, an interoperable and minimalistic compliance regime is important in terms of avoiding regulatory hassles and bureaucratic delays. Similarly, the rights-based approach and digital inclusion are important from a human rights perspective and ensure the basic protection of citizens' data. Therefore, following are some of the factors that should be considered while entering into a principle-based data-sharing agreement.

## 6.1. INTEROPERABLE DATA PROTECTION REGIME

Data interoperability is one of the most crucial factors for a smooth flow of cross-border data and ensures the efficient functioning of data-driven businesses. Interoperability, as a concept, is generally construed as a mechanism for computer systems from two different organisations to work together.<sup>159</sup> Over the years, interoperability has evolved. For example, interoperability in India's Unified Payment Interface (UPI) is one of the most successful examples from technical standpoint. The way it functions across platforms has enabled the free flow of payments in the country. However, with emerging data-driven businesses and the globalised world where frequent transfers is a norm, it must be noted that it should not only be limited to its technical construction but must be extrapolated into the regulatory sense as well. Regulatory interoperability allows for that there is synergy between the laws and regulations of two countries at an international level.

With increased data transfers, the data protection regulations of different countries should be harmonised to facilitate data transfers. While there is a general consensus on the core principles of data protection across the world, various countries have regimes that conflict with each other. An ideal regulatory approach could be that having minimal fewer restrictions on cross-border data transfers along with strong domestic safeguards to protect personal data is the most conducive environment to grow trade in digital services.<sup>160</sup> A principle-based framework could enable regulatory interoperability and in turn, enable cross-border data flow.

<sup>158</sup> OECD/G20 Inclusive Framework on Base Erosion and Profit Shifting, Retrieved from: <https://www.oecd.org/tax/beps/about/>

<sup>159</sup> Brown, I. (2020, July 30). *Interoperability as a tool for competition regulation*. CyberBRICS. Retrieved March 21, 2022, from <https://cyberbrics.info/wp-content/uploads/2020/08/Interoperability-as-a-tool-for-competition-regulation.pdf>; See also, Tripathi, A., Shekar, K., Venkatesh, K., & Misra-Elder, M. (2022). *Harmonising the UK and India Data Protection Regime*. The Dialogue. <https://thedialogue.co/wp-content/uploads/2022/03/HARMONISING-THE-UK-AND-INDIA-DATA-PROTECTION-REGIME-The-Di-ologue-UKIBC.pdf>

<sup>160</sup> Ferracane, M. F., & Marek, E. v. d. (2021, March). *Regulating Personal Data: Data Models and Digital Services Trade*. World Bank. Retrieved March 21, 2022, from <https://openknowledge.worldbank.org/bitstream/handle/10986/35308/Regulating-Personal-Data-Data-Models-and-Digital-Services-Trade.pdf>

Trust building between India and other jurisdictions must be along the lines of looking out for principles like confidentiality, data protection and security within the domestic legislation. These principles form the bedrock for a safe and secure data protection regime. These elements protect the basic sanctity of data and ensure that the privacy and security of the datasets are maintained. This trust needs to be developed in regard to the entities controlling the data and should be undertaken by the government.<sup>161</sup> Seeking out principles for trust building is crucial for India to allow the government to create a friendly policy environment for local and international investment.<sup>162</sup> The individual trust would lead to more willingness in terms of data sharing, which would allow the fiduciaries to participate in cross-border data transfers. Furthermore, India may also look out for data provenance provisions in recipient jurisdictions and place the burden on data exporters to ensure the integrity of data.<sup>163</sup> Data provenance refers to the trail that accounts for the origin of a piece of data with an explanation of how and why it got to the present place.<sup>164</sup> This would help in building trust in the recipient jurisdictions and also foster accountability.

India must look for consumer protection principles in terms of having a redress mechanism institutionalised by the recipient country. However, in order to address issues at their national levels, governments should be free to adopt measures suited to their needs.

India's experiment with interoperability has been currently limited to domestic frameworks. It has come out with several policies to enable interoperability at the national<sup>165</sup> and sectoral levels.<sup>166</sup> On the technical front, the Unified Payment Interface (UPI) has been a successful model for interoperability, and similar success is envisioned for Open Network for Digital Commerce (ONDC) as well. However, if it is to become a global technology hub, harmonising the regulations must be managed with other data protection regimes in mind. The exchange of data is crucial for growth and innovation. For facilitating seamless data flows between countries, interoperability and harmonisation of laws at the principle level with other jurisdictions is important.<sup>167</sup>

## 6.2. MINIMALISTIC COMPLIANCE REGIME

A jurisdiction with high standards of ease of doing business having a minimalistic yet narrow and focused compliance regime should be one of the priority areas for India to negotiate with the other jurisdictions. India, must look out for how businesses of two different sizes, activities and risk levels are approached by the other jurisdictions under their regulation appropriately. Besides, India can push for a scale-based approach for data compliance during government negotiations which is calibrated horizontally, i.e., depending upon the size of the business and vertically, i.e., sector, size of the risk and sensitivity of the data processed. Thus, considering calibrating the data protection mandate optimally would allow start-ups and MSMEs to enjoy light-touch regulation and aid their development. However, it would be necessary for the government of the other jurisdictions to determine the buckets and threshold based on size, sector and risk in a participatory

<sup>161</sup> Report for the G20 Digital Economy Task Force, "Mapping Approaches To Data And Data Flows" (SAUDI ARABIA, 2020) OECD. Available At <https://www.oecd.org/sti/mapping-approaches-to-data-and-data-flows.pdf>

<sup>162</sup> Ibid.

<sup>163</sup> World Economic Forum, "A Roadmap for Cross - Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy" White Paper World Economic Forum (June 2020) Available At: [https://www3.weforum.org/docs/WEF\\_A\\_Roadmap\\_for\\_Cross\\_Border\\_Data\\_Flows\\_2020.pdf](https://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf)

<sup>164</sup> Gupta, A. (2009). Data Provenance. In: LIU, L., ÖZSU, M.T. (eds) Encyclopedia of Database Systems. Springer, Boston, MA. [https://doi.org/10.1007/978-0-387-39940-9\\_1305](https://doi.org/10.1007/978-0-387-39940-9_1305)

<sup>165</sup> Examples include - National Open Data Ecosystem

<sup>166</sup> Examples include: National Digital Health Mission (NDHM), Open Network for Digital Commerce (ONDC), Unified Payment Interface (UPI)

<sup>167</sup> *Data Localisation In A Globalised World: An Indian Perspective*. (2018, November 18). The Dialogue. Retrieved March 21, 2022, from [https://thediologue.co/wp-content/uploads/2020/01/Data-Globalisation-in-a-Globalised-World-copy\\_compressed.pdf](https://thediologue.co/wp-content/uploads/2020/01/Data-Globalisation-in-a-Globalised-World-copy_compressed.pdf)

manner involving stakeholders like industry associations, businesses etc.

Also, India must look out for how other jurisdictions are bridging the capacity concerns by complying with data protection mandates, whereas India may push other jurisdictions to encourage businesses to use privacy-enhancing technology by incorporating it with their domestic data protection regulations. Therefore, these negotiations must form a minimalistic compliance regime to have optimal data protection practices.

## 7. CONCLUSION

In a globalised world, the internet and technological developments have paved the way for the emergence of data-driven business models that value data in economic terms. This development has transformed the goods and services trade which is increasingly digital and dependent on the free flow of data across borders. As data is becoming a yardstick for international trade, it is important for India to consider frameworks to enable the free flow of data across borders.

To stress the need to enable the free flow of data and to develop critical technology standards in the long run, in this report, we attempted to bridge the gap in the existing literature around data transfers. In this report, we proposed a principle-based framework that India can enter with other jurisdictions to enable the free flow of data.

In this report, we considered the differences in the interests and developments in India and other jurisdictions in terms of laws, practices, priorities and their relationship with other countries. While regulatory and legislative differences between jurisdictions are inevitable, we propose that mutual recognition of core principles of data protection, privacy, and security through bilateral/multilateral frameworks will enable the interoperability of data protection regimes.<sup>168</sup>

Besides adding to our objective of consensus building, the principle-based framework proposed through this report provided a balance of differences in national constraints and practices while respecting international principles to harmonise data regulation regimes for seamless implementation.

Therefore, we believe that the seamless implementation of a principle-based cross-border data transfer framework will create a trusted environment for countries to enable data transfers, which will minimise the business compliance cost and unlock various potentials.

---

<sup>168</sup> Charlet, K., Sauer, R., Nelson, M., & Jain, R. (2021). Fragmentation: The future of the geopolitics of Data. (M. Raghavan, Moderator) Retrieved from Carnegie India





# 8. ANNEXURE 1

## LITERATURE REVIEW

We analysed various approaches countries have taken in their data regulations covering (a) Asian countries like India, China, Japan, Singapore, Philippines, Thailand, South Korea, and Bangladesh, (b) European countries like GDPR, Russia, UK (c) North American countries like the US, Mexico, Canada (d) South American countries like Brazil, Argentina, Columbia (e) African countries like South Africa, Rwanda, Ghana, Kenya, Morocco, Uganda (f) Oceania countries like Australia, New Zealand.

Please [click here](#) or scan for our detailed review.





# 9. ANNEXURE 2

## METHODOLOGY

**Sampling Strategy:** The study adopted a non-probability sampling by selecting respondents for input in a non-randomised manner. Also, we adopted snowballing sampling, where some of our respondents put us in touch with other potential respondents. The study is based on primary research with inputs from industry stakeholders from India to understand multiple viewpoints and concerns around restricting cross border data flows. As tabulated below, we received 25 inputs from various stakeholders, predominantly from start-ups and cloud service providers/data processors.

**Data Collection Method:** We adopted a semi-structured interview design to seek input from the stakeholder holders where all our stakeholder interviews were conducted virtually. Also, some of the respondents chose to share their input by filling out the online questionnaire.

**Data Analysis Method:** Our engagement with stakeholders provides us with a rich source of information on how data localisation and restrictive cross-border data transfers would impact the start-ups and data processors/cloud service providers. We adopted the thematic analysis technique, where we analysed the themes within the data set to identify meaning. Identified themes focus on the key aspects that relate to our research questions.







The Dialogue™

INFORM ENGAGE IDEATE



<https://thedialogue.co>

**Recommended Citation :** *Shekar, K., Tripathi, A., Birla, B., & Vaidya, E. (2022). Principle-based Framework Towards Cross-Border Data Transfers. The Dialogue*

The Dialogue™ is a public-policy think-tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue™ has been ranked as the world's Top 10 think-tanks to watch out for, by the Think-Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.