UK INDIA
BUSINESS COUNCIL

JULY 2023

PATHWAYS FOR A UK-INDIA DATA BRIDGE

INTRODUCTION

The Digital Personal Data Protection Bill, 2022 (DPDPB 2022), released in 2022 for consultations, paves the way for a simplified, principle-based framework to govern personal data in India. This Bill also provides a principle-level congruence in data protection regimes between two of the world's leading digital services suppliers, India and the UK, and facilitates a positive environment to expand digital trade between both countries.

As India finalises the Data Protection Bill for introduction into law, UK India Business Council have undertaken on a range of policy discussions on the Bill including a report last year on 'Harmonising the UK and India data protection regimes' as well as submissions to the Government of India on the recent iterations of the Bill.

In this context, we are pleased to share our report on "**Pathways for a UK-India Data Bridge**" prepared along with our knowledge Partner, **The Dialogue** – an emerging research and policy think-tank. The report contains perspectives of Indian and UK businesses on approaches to enabling cross-border data transfers, especially between India and the UK, coexisting models of both bilateral and transnational cooperation on enforcement aspects, ensuring coordinated efforts with key sectoral regulators where data governance provisions will interplay, and other related aspects.

To discuss the key implications emerging from the Bill, UKIBC organised a UK-India Data Roundtable on the Draft Digital Personal Data Protection Bill, 2022 in April 2023. For this discussion, we were joined by Mr. Baijayant Panda, National Vice President-BJP, a key advocate on data privacy reforms. We were joined by representatives from the British High Commission in India, experts who have worked with government and think tanks and our member companies across sectors such as defence technologies, financial and professional services, information and communication technology (ICT) services, among others.

This report presents an analysis on the UK and India data protection regimes as well as key recommendations for the final version of the Digital Personal Data Protection Bill.

KEY IMPERATIVES ON INDIA'S DATA PROTECTION REGIME

As India has moved towards adoption of the Data Protection Bill over the past years, there have been several transformational shifts in digital governance, with the adoption and usage of technological innovations like Digital Public Infrastructure for service delivery. India is also evolving itself from being an adopter of technology to creating technology which is scalable and complements the ecosystem. The following section outlines the perspectives and key suggestions that have emerged from industry members as part of recent conversations including the Data Roundtable held in April 2023 with Mr Panda:

India's position on data in trade agreements and UK-India cooperation:

India's stand on cross-border data transfers has evolved over time with two key recent developments: (a) the Free Trade Agreement (FTA) with the United Arab Emirates marked the first Indian FTA that had a section on the Cross-Border Flow of information within the digital economy chapter. (b) Joint Declaration on Privacy and the Protection of Personal Data with European Union, Australia, Comoros, Japan, Mauritius, New Zealand, the Republic of Korea, Singapore, and Sri Lanka.

India and the UK have vibrant start-up ecosystems with strong digital and technology sectors in particular. India has the world's third largest start-up ecosystem and is well regarded among global peers for its strong technology presence, including among its 100 'unicorns' (start-ups with a value of greater than USD 1 billion). The UK's tech sector became just the third country sector to reach USD 1 trillion in value milestone in 2022 and UK start-ups, universities and global corps are regarded among the world's best.

Accordingly, India and the UK have significant complementarity in terms of strengths as digital service suppliers and therefore, could mutually benefit from enabling cross-border data transfers, including through bilateral arrangements that facilitate the free flow of data.

Enabling trusted data flows:

Our members find that the proposed concept of 'trusted geographies' where the data transfer will be permitted provides an appropriate balance between economic goals and security concerns. The Government of India could consider a tiered or graded approach for nations with lower data security standards from the list while allowing free data flows with geographies that have the requisite protection standards.

Whitelisting countries could be a reasonable way to determine permissibility of Indian citizens' data flow outside its territory. The Government could keep expanding the whitelist as a dynamic list as appropriate over time.

While evaluating the notification of the countries, India could adapt the parameters of "trusted partners" as set out in other regional groupings such as the QUAD etc., to enable the free flow of data provided the trusted partners reciprocate the same in terms of allowing their citizen's data to flow to India. However, here the term “trust” in the trusted partner concept needs to be elaborated keeping specific parameters in mind, given it is different from Data Free Flow with Trust principle enumerated in G20 Osaka declaration.

To ensure reciprocity, it was suggested that the data protection pact must be part of bilateral and multilateral agreements similar to the India-UAE Free Trade Agreement, where data protection standards and the importance of cross-border data transfers were discussed as part of the digital economy chapter.

Besides notifying countries, at the operational level, industry members would welcome a principles-based framework between India and trusted partners (countries like the UK) where data protection and security principles are mapped to various players within the data lifecycle across borders. For instance, specific principles mapped to data fiduciaries (Data exporters and Data importers), intermediaries, data processors and data centres etc.

For example, Data exporters are expected to follow principles such as consent and notice, collection limitation, purpose specifications, data quality, data principals/subject’s rights, simplicity, and legality. Data Importers must follow principles such as baseline scope, compliance, security, data breach notification, accountability, and data expunction.

The DPDPB 2022 allows the Central Government to determine the necessary factors for notifying countries on permissibility of cross-border data transfers. However, the factors which would be taken into consideration have not been made clear. Our members would welcome clearly defined criteria to ensure there is greater transparency and accountability streamlined in the process.

Our members find that the principles-level conversation could act as a means to initiate a negotiation between India and the UK in terms of enabling data flow and digital trade partnerships through consensus building.

While data protection is approached differently by India and UK to cater to their respective domestic concerns and needs, the cross-jurisdictional analysis of data protection regulations shows there is potential for a principle-level congruence between India and the United Kingdom on key aspects.

For instance, India’s upcoming DPDPB 2022 is guided by some of the first order data protection principles accepted globally like storage limitation, data minimisation, purpose limitation etc. Similarly, the UK also shares these principles within its data protection regulation and is based on key principles: fair, lawful, and transparent processing; purpose limitation; data minimisation; accuracy, storage limitations; Data security, and accountability.

This similarity, at the principles level, can act as a means to initiate a conversation between India and the UK in terms of enabling data flow and digital trade partnerships through consensus building.

Therefore, the principle-based framework would bring a nuanced and holistic approach to cross-border data transfer mechanisms within the business-related data transfers (B2B) chain. It proposes a systematic approach to cross-border data transfer mechanisms, where principles will be a prerequisite for various kinds of business-to-business data transfer chains.

Widely accepted principles such as 'Privacy by Design', fair and lawful processing, purpose limitation, and data minimisation to be followed by third parties, data processors and cloud service providers who are stationed in other jurisdictions could be embedded into the framework.

A principle-based approach suggests that 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.

While most of the models and mechanisms are concerned with end players, it is important to have a holistic approach to cross-border data transfer where the principles such as data-in-motion security, coordination, and data anonymity commend go-between players' compliance and end players.

Besides, some of the globally accepted principles such as balanced discretion, consistency test, choice of jurisdiction, data-based policy goals, collaborative formulation, and recognition of accountability could be considered by the domestic regulators and governments in enhancing international-level coordination and cooperation.

Therefore, while notifying countries would be one way to facilitate cross-border data transfers, it was highlighted that the government may consider other existing mechanisms followed by the businesses, such as:

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.

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 trust marks/certificates as a valid mechanism to facilitate cross-border information transfers while protecting personal information.

(b) Codes of conduct: This 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. Thus, these codes reflect the processes and functions of the data fiduciaries (within the industry) that had signed. The UK tests these mechanisms as part of its post-Brexit data transfer arrangements.

(c) 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. Both countries ensure that data holders and data recipients sign BCR.

(d) 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 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. For instance, the EU and the UK have recognised or issued Standard Contractual Clauses. Similarly, the Association of Southeast Asian Nations (ASEAN) has recognised model contractual clauses for data transfers.

Therefore, as India moves towards enabling cross-border data transfers, it could consider a combination of the above-discussed mechanisms (some of which are already well established in the UK) tailored to embed some of the key data protection principles across the pipeline.

Regulatory Capacity for Adequate Implementation

From India's data protection bill's perspective, industry members consulted suggest establishing a separate and independent data regulator with adequate regulatory capacity to govern, while maintaining regulatory coordination across sectors where appropriate (especially in financial, telecom services, etc.)

In situations where a conflict of interest may arise for Government of India, which may act as a data fiduciary under certain circumstances, a supplemental grant of responsibility of a regulatory body on the Data Protection Board is suggested rather than being limited solely to adjudicatory functions. This would be along similar lines to the roles played by regulators such as the Securities and Exchange Board of India or the Competition Commission of India.

The Data Protection Board, as envisaged under the DPDPB 2022, assumes a quasi-judicial role. However, the DPDPB 2022 lacks explicit provisions concerning the institutional and functional independence of the Data Protection Board such as the processes for selection and removal of members. Safeguarding against such concerns necessitates incorporation of statutory safeguards that guarantee both functional and institutional independence to the Data Protection Board.

Similarly, our members believe that India could evaluate equivalent safeguards being provided to foreign citizens' data with Clause 18 (1)(d) of Digital Personal Data Protection Bill 2022. While India's data protection regulations provide the utmost safeguards to data of persons resident within the territory of India, however similar protections are not provided to foreign citizens.

It is also perceived that data protection regulation and enforcement fall under the ambit of multiple regulators domestically, and there is a need for domestic-level consensus building through establishing inter-regulatory coordination. There is a need for harmonisation with other statutes and regulatory bodies dealing with or functioning at the intersection of digital personal data with the respective subject matter.

Law Enforcement Access and Security Considerations

A key sticking point and a reasoning behind the need for data localisation has been the delay in accessing Indian citizen's data stored offshore for law enforcement purposes. The challenge arises from the broke MLAT process and Budapest convention process, which lacks agility.

Therefore, businesses request that India seeks assurance from its key trading partners that Indian citizens' data will be provided to the Government of India in an agile fashion such that there is no delay in critical investigations.

Businesses also contend that data localisation may not be the answer to providing greater law enforcement access and addressing national security considerations. Instead, countries may work towards building a trust-based framework on upholding common standards and safeguards on government access to personal data for law enforcement purposes.

In this regard, the - OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, which is touted as the "first intergovernmental agreement on common approaches to safeguarding privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes" can be a useful point of reference.

This Declaration acknowledges that OECD countries should adhere to shared principles and safeguards regarding government access to personal data and strongly opposes any approach to such access that conflicts with democratic values and the rule of law.

FOUR RECOMMENDATIONS FOR INDIA'S DATA PROTECTION REGIME

1. Harmonising Reciprocal Arrangements

To ensure reciprocity of similar data protection regimes, India could look at a digital chapter in its ongoing and future trade negotiations along similar lines to the India-UAE Free Trade Agreement, where data protection standards and the importance of cross-border data transfers were discussed as part of the digital economy chapter.

New institutional mechanisms with more permanence that convenes senior government officials and high-level representatives of multiple stakeholder groups could be established. India's G20 Presidency moment could establish an Institutional Partnership to facilitate principles behind cross-border data cooperation.

For example, at the recent G7 meeting, an Institutional Arrangement for Partnership (IAP) was announced to advance data free flows with trust.

2. Provide Due Recognition to existing Data Transfer Mechanisms

As seen with other mature jurisdictions, India could consider allowing use of other enforceable tools such as Binding Corporate Rules and model contract clauses (for example, EU standard contractual clauses) to enable cross-border data flows.

Standard contractual clauses and binding corporate rules based on frameworks such as the APEC Privacy framework and Cross Border Privacy Rules (CBPR) should be taken into consideration as legitimate grounds to processing personal data under the Bill.

3. Ensuring a Converged Approach where sectoral data regulations apply

As various sectoral regulations such as the RBI on digital lending or the telecom authority on conditions for unified license may carry differing obligations for industry players, a mechanism of ensuring regulatory convergence may be considered to ensure that added compliance burden is not imposed on the industry in sectors such as financial services, telecom, etc.

4. Driving Consensus on trust-based standards for data sharing on law enforcement access

India could look to build a trust-based framework on upholding standards and safeguards on government access to personal data for law enforcement purposes. In this regard, the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, could be looked at, when accessing personal data for national security and law enforcement purposes as a useful point of reference.

ANNEXURE

COMPARISON OF DATA PROTECTION REGIMES: THE UK AND INDIA

UK Model	Indian Model	Industry Suggestions
The responsibility of holding two key rights of the individuals, i.e., information rights and the right to data privacy, is housed within a single regulator, i.e., Information Commissioner's Office.	The information rights and right to privacy have been handled separately in India, where we have an information commissioner and envisioned Data Protection Board (Adjudicatory body) for respective purposes	**As information rights and the right to privacy are two sides of the same coin, India could consider evaluating approaches from the UK model while analysing compatibility and harmonisation in the Indian context.**
Under Article 51 of the UK GDPR, the Information Commissioner Office (ICO) is set up as a supervisory authority to enhance the bill.	The previous versions of India's data protection bill had a provision for establishing a separate Data Protection Authority as a supervisory authority, but DPDPB 2022 has removed such a provision. While there will be Data Protection Board, it would only act as an adjudicatory body.	**India could look to consider the merits of an independent data regulator with adequate regulatory capacities, whilst maintaining regulatory coordination across sectors (such as financial, telecom services) where appropriate.**

UK Model	Indian Model	Industry Suggestions
Sections 74 (a) and 74 (b) of Chapter V of the Data Protection Act 2018 provide the adequacy standards for the international transfer of data. It requires the third country to be a privacy-respecting and a rule of the law-based state, respecting human rights and freedoms.	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.	**The UK and India could work closely and collaboratively for a Data Adequacy Agreement based on reciprocity in economic, data and security principles. The best practice dialogue between the UK authorities and ICO with the Indian authorities may be institutionalised along with other key stakeholder groups.**
The UK, under UK GDPR and Data Protection Bill 2018, extends the same level of data protection safeguards provided to its citizens to foreign citizens' data travelling to the UK.	Clause 18 (1)(d) of DPDPB 2022 provides differential level of data protection safeguards provided to Indian citizens and to the foreign data principals.	**India could evaluate equivalent safeguards being provided to foreign citizens' data with Clause 18 (1)(d) of Digital Personal Data Protection Bill 2022.**

UK INDIA
BUSINESS COUNCIL

The UK India Business Council is a strategic advisory and policy advocacy organisation with a mission to support businesses with insights, networks, policy advocacy, services, and facilities needed to succeed in the UK and India. We believe passionately that the UK-India partnership creates jobs and growth in both countries, and that UK and Indian businesses have ideas, technology, services and products that can succeed in India and the UK respectively.

www.ukibc.com

UK INDIA BUSINESS COUNCIL
LONDON
25 Wilton Road
London SW1V 1LW
United Kingdom
Tel: +44 (0)20 7592 3040

UK INDIA BUSINESS COUNCIL
GURUGRAM
WeWork, DLF Forum, Cyber City,
Phase III, Sector 24,
Gurugram 122002,
Delhi-NCR
Tel: +91 (0) 124 502 6059

PATHWAYS FOR A UK-INDIA DATA BRIDGE

For more about our Digital Sector work at UKIBC, you can connect with Subhodeep Jash at subhodeep.jash@ukibc.com