The Dialogue™
INFORM ENGAGE IDEATE

UK INDIA
BUSINESS COUNCIL

MARCH 2022

REPORT

HARMONISING THE UK AND INDIA DATA PROTECTION REGIME

Ayush Tripathi | Kamesh Shekar | Karthik Venkatesh | Meghna Misra-Elder

AUTHORS

Ayush Tripathi

Senior Research Associate

His area of interest are regulations surrounding Technological Advancements, International Law and Human Rights. During the course of his term at the organization, he has worked on a wide array of empirical project including but not limited to increase of export competitiveness of electronic manufacturing industry, taxation, data privacy and e-commerce sector.

Kamesh Shekar

Senior Research Associate

His area of research covers informational privacy, surveillance technology, intermediary liability, safe harbour, issue of mis/disinformation on social media, AI governance, etc.

Karthik Venkatesh

Programme Manager

He is the programme manager for the data governance and data flows vertical. Currently, he is working on copyright and IPR issues with data sharing in the digital economy, impact assessment of regulations relating to personal and non personal data flows on startup ecosystem, and the future of a sharing economy.

Meghna Misra-Elder

Associate Director

Meghna's role supports members in the Life Sciences & Healthcare and Digital Innovation sectors carrying out strategy development, client relationship management, delivering member services, top level business engagement, supporting UK and Indian companies' with their trade and investment activities, and identifying new business opportunities.

Editor: Kazim Rizvi

Research Assistance: Bhavya Birla

Designed by: Divya Vishwanathan, Diksha Kumari

**All authors are listed in alphabetical order.*

Executive Summary

Across the world, countries are trying to unlock the economic potential of data. Data accessibility, usability and availability will be key to achieving this potential. In a globalised world, this means that enabling the free flow of data across borders will be critical. The United Kingdom (UK) and India are two such countries that are working towards unlocking this potential on a larger scale. Although the benefits that can be derived from data transfers are plenty, governments have been historically concerned with the privacy and security implications of such transfers in the absence of protection frameworks and regulated mechanisms. While the UK has a full-fledged data protection law and a data protection authority, India is at the cusp of enacting a historic data protection law after years of deliberations.

Interoperability[1] and harmonisation[2] of data protection laws between the two countries are essential to the growth prospects of both nations. Existing methods of data transfer (transfer of data between two countries), which takes place through the Standard Contractual Clauses (SCCs), is a complex process, filled with bureaucratic compliances. These approvals are done on a case by case basis, and have to be approved for every transfer. Interoperability would help smooth the transfer of data and reduce regulatory hurdles. The alternative, which allows for seamless data transfers outside of supervisory approval can be achieved through an adequacy finding. The UK requires adequacy criteria to be met to protect citizen's data in the second country. Adequacy, in this context would mean 'essentially equivalent' level of data protection to that which exists within the UK.

[1] UK and India's data protection regulations (two distinct framework) must find ways to communicate and interact with each other.
[2] Process through which the UK and India can create common and uniform data protection principles, standards etc.

In India, the latest draft of the personal data protection bill, although making significant strides towards adequacy, has room for greater alignment. Issues relating to the independence of the data protection authority and exemptions given to the government for processing data in the current draft of the Personal Data Protection Bill are among the key challenges that may restrict India from meeting international adequacy standards. Further, non-personal data should be excluded from the personal data protection bill as most jurisdictions do not regulate personal and non-personal data together.

Digital trade[3] through goods and services has been on the rise for both nations. To maximise the benefits and achieve the full potential of the India-UK digital trading relationship a bilateral data transfer agreement could help the seamless flow of data between the two countries. The ongoing India-UK FTA negotiations present both governments an opportunity to create a data transfer framework that can enable seamless data flow to facilitate economic growth and innovation in both countries.

In this report, we highlight the importance of having an interoperable and harmonised data protection regime for India and the UK in order to facilitate the free flow of data and wider digital trade. **Chapter 1** provides background and short introduction to the data protection regimes in the UK and India. **Chapter 2** delves into interoperability and its advantages. **Chapter 3** highlights the potential roadblocks to a data transfer agreement, and **Chapter 4** provides a way forward that will deliver an interoperable regime.

[3] Digital trade has been discussed by OECD as - *"While there is no single recognised and accepted definition of digital trade, there is a growing consensus that it encompasses digitally-enabled transactions of trade in goods and services that can either be digitally or physically delivered, and that involve consumers, firms, and governments." See more - OECD, The impact of Digitalisation on Trade,* Retrieved from: https://www.oecd.org/trade/topics/digital-trade/.

About

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, in 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.

UK India Business Council (UKIBC) is the leading trade organisation solely focussed on promoting bilateral economic relations between the UK and India. Structured as a not-for-profit organisation, we are an independent, business-led and Government backed knowledge partner with unique networks and contacts in the Indian and UK public and private sectors. We support our stakeholders, members and clients in achieving their goals through strategic advisory and policy advocacy services, working with stakeholders across the UK and Indian Government, including State Governments in India as well as central, devolved administrations, and city regions in the UK.

TABLE OF CONTENTS

1. BACKGROUND

Digital trade has opened a wide range of opportunities that extend beyond geographic borders. In addition to expanding the markets in which to conduct business, data transfers are increasingly becoming vital for innovation, operational ease, and economic activity in the digital and related space.

In 2018, the UK exported £190 billion in services delivered digitally. While, in 2019, investments in the UK tech sector soared to £10.1bn – a £3.1bn increase on 2018 and the highest level in UK history.[4] Data transfers have become crucial for boosting productivity and trade, supporting new businesses and jobs, increasing the speed, efficiency and scope of scientific research, and for driving better delivery of policy and public services.[5] The figure below extracted from the OECD report shows the data revenue generation by different businesses internationally[6] by monetising data. Similarly in India, there have been multiple documents that allude to the value of data and its close linkage with economic activity.[7]

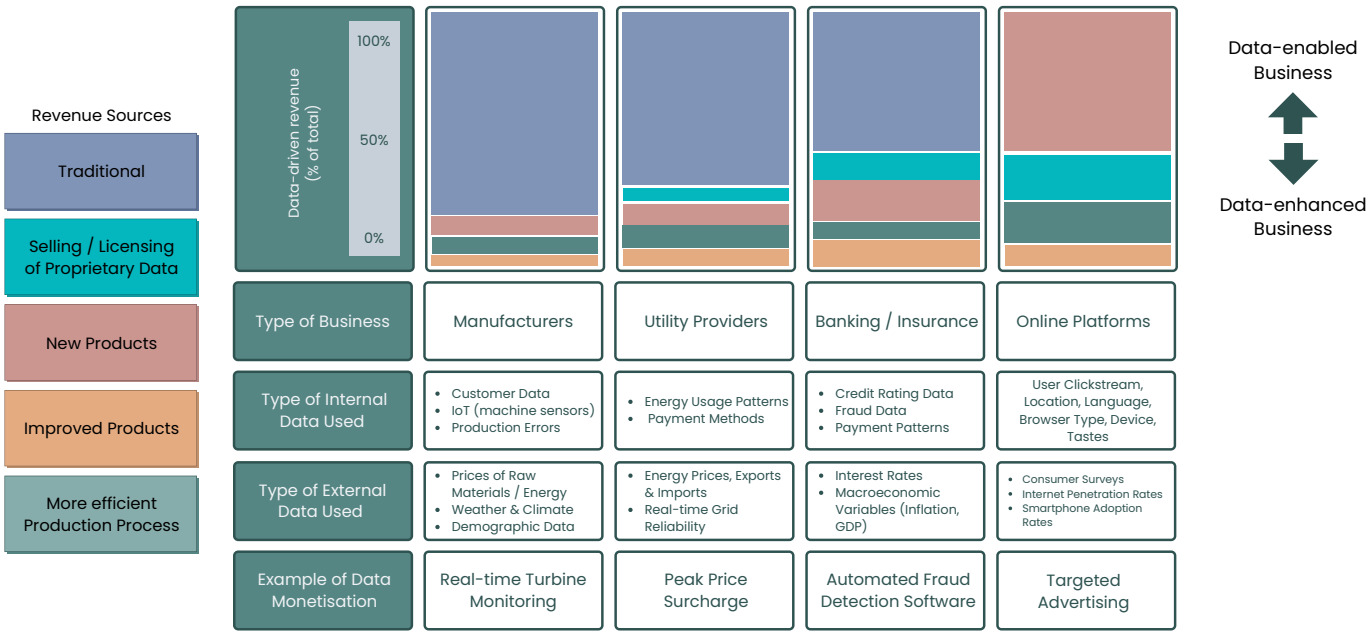

Figure 1: Data monetisation across business models and sectors [Source: OECD Report[8]]

[4] *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-data-transfers/international-data-transfers-building-trust-delivering-growth-and-firing-up-innovation.

[5] *UK National Data Strategy*. (2020, December 9). GOV.UK. Retrieved March 21, 2022, from https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#the-data-opportunity.

[6] The report analyses global value chain of data through culmination of various secondary research.

[7] *Report by the Committee of Experts on Non-Personal Data Governance Framework*. (n.d.). Ministry of Electronics and Information Technology. Retrieved March 21, 2022, from https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf; *India Data Use and Accessibility Policy*. (n.d.). Ministry of Electronics and Information Technology. Retrieved March 21, 2022, from https://www.meity.gov.in/writereaddata/files/India%20Data%20Accessibility%20and%20Use%20Policy.pdf.

[8] *Measuring the Economic Value of Data and Data Flows*. (2020, August). OECD Digital Economy Papers. https://www.oecd-ilibrary.org/docserver/6345995e-en.pdf?expires=1647502699&id=id&accname=guest&checksum=39C6362567659687C59423DD656B9A5B.

India is moving towards a comprehensive data protection regime with the proposed Data Protection Bill, which was first introduced in 2018. Over the years, there have been multiple iterations of the Bill as it has gone through a rigorous consultative process. Yet, while there are certain aspects of the Bill that stand the test of global data protection standards, there are avenues to further enhance the cooperation between countries as far as regulatory regimes are concerned.

The seamless flow of data across the border is crucial to enable innovation, economic proliferation, and competition through digital data serivces. In addition, the free flow of data can particularly help the MSME sector and start-ups by expanding and enabling access to the global supply chain and breaking entry barriers.[9] Therefore, policy and regulation need to evolve in close connection with the new models of business and innovation, to ensure that we continually benefit from the novel opportunities.

As India is on its path to achieving the trillion-dollar digital economy target, it is ideal for enabling cross-border data flow through bilateral/multilateral arrangements, especially with the United Kingdom, due to its trade value.[10] Moreover UK's National Data Strategy[11] recognises the importance of international free flow of data for enhancing its digital service export which stood at £190 billion in 2019.[12]

Traces of Interoperability and Harmonisation in Regulations

The first attempt at harmonisation can be traced back to regulations on trans-border data flows in Europe in the 1970s. In the 1980s, the OECD formulated guidelines on data flows, data protection and privacy. After realising the efficiencies that can be achieved through the free flow of data across the borders, there have been moves towards harmonisation of data governance regimes across the world. While there is general consensus for the core principles of data protection across the world, various countries have regimes that conflict with each other.

In a recent paper by the World Bank[13], it was found that a regulatory approach

9 *Tripathy, A., Venkatesh, K., & Pande, T. (2021, January 6), Impact Report: Personal Data Protection Bill on the Startup Ecosystem.* The Dialogue. Retrieved March 21, 2022, from: https://thedialogue.co/wp-content/uploads/2021/01/Startup-Report-Final-Document-vF.pdf.

10 It is estimated that bilateral trade value between India and UK will reach USD 100 billion by 2030.

11 *UK National Data Strategy*. (2020, December 9). GOV.UK. Retrieved March 21, 2022, from https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy.

12 *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-data-transfers/international-data-transfers-building-trust-delivering-growth-and-firing-up-innovation.

13 Ferracane, M. F., & Marel, 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.

that has 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. Further, countries with compatible data processing and transfer regimes tend to have a higher level of digital services trade between them as compared to trading partners with different data regimes.[14] There is a need for an interoperability mechanism that would improve efficiency and add value to businesses and governments without compromising the informational privacy rights of users.

The UK has a robust data protection law in place, which was arrived at after years of consultation. The UK implemented the EU Data Protection Directive through the Data Protection Act in 1998. It has been amended several times since and has now given way to UK General Data Protection Regulation (GDPR). At this crucial juncture, when India is seeking to finalise its domestic regime, including provisions regarding interoperability, understanding the UK's journey to implement the law can be a useful learning experience for a smooth transition. Moreover, the ongoing Free Trade Agreement talks between the two nations give an added impetus to discuss and align aspects relating to data and digital trade.

Interoperability in a traditional sense is a mechanism for computer systems to work together even if they are from different organisations.[15] However, with digital markets constantly evolving, interoperability can also be construed on two fronts. First is the traditional technical interoperability and second is the regulatory interoperability. Technical interoperability, as defined above, is the mechanism for systems of even competing companies to work together. An example of interoperability in this sense could be India's Unified Payment Interface (UPI) systems. Regulatory interoperability on the other hand means that there is synergy between laws and regulations of two countries at an international level or between two or more departments at a domestic level. Having an interoperable regime helps to smooth transfer of data and avoids regulatory hassles. Since this report delves into data transfer between two countries, a suitable example of interoperability at an international level would be an agreement between India and the UK for data flow. This would help companies in both countries, especially multinational companies, to transfer data seamlessly.

India's experiment with interoperability has been currently limited to domestic frameworks. However, if it is to become a global technology hub, interoperability has to be managed with other data protection regimes in mind. Exchange of

[14] Ibid

[15] 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.

data is crucial for growth, innovation and for law enforcement purposes. For facilitating seamless data flows between countries for the aforementioned purposes, harmonisation of laws with preferred foreign jurisdictions is important.[16]

It is pertinent to note that India has the 2nd largest startup ecosystem in the world; expected to witness Y-o-Y growth of 10-12 per cent or ~20,000 startups. Around 4,750 of these are technology-led startups. In fact, 1,400 new tech startups were born in 2016 alone; implying there are 3-4 tech startups born every day.[17] Moreover, the pandemic has accelerated the growth with an increased thrust on most services going online. The regulators in India have been working towards creating a facilitative environment for startups to thrive and expand through initiatives such as regulatory sandboxes, innovation sandboxes, exemptions, incubation centres and priority sector lending that allows for greater ease of doing business.

However, lack of knowledge impacts collaboration, particularly in the case of start-ups and SMEs which may not be aware of the benefits of overseas collaboration and may be restricted in scaling in a global market. Regulatory uncertainty and lack of technical support also act as hurdles for resource-constrained SMEs with global ambitions. When considered that the number of SMEs in India currently stands at 3,26,514,[18] we feel this is a missed opportunity for growth and innovation, as SMEs form the backbone of the economy.

Against this backdrop, this report analyses the key roadblocks that may come in between harmonising the UK and India's data protection laws and ultimately to improving collaboration between the countries. It will further elaborate on some strategies that India could use towards future data regulation to enhance interoperability with the UK and by extension with other countries as well.

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

[17] *Indian Startup Ecosystem*. (2022, February 25). Startup India. Retrieved March 21, 2022, from https://www.startupindia.gov.in/content/sih/en/startup-scheme/International/indian-startup-ecosystem.html.

[18] *MSME Industry in India – Market Share, Reports, Growth & Scope*. (2021, December 17). IBEF. Retrieved March 21, 2022, from https://www.ibef.org/industry/msme.aspx.

2. INDIA AND UK DATA PROTECTION LAW: LAYING OUT THE LANDSCAPE

The UK had adopted GDPR by virtue of ***section 3 of the European Union (Withdrawal) Act 2018***,[19] as amended (including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ('UK GDPR'), and the Data Protection Act 2018. India, on the other hand, is working on its domestic regulation. This section presents an overview of the key provisions of the data laws in these two countries.

2.1. United Kingdom

The UK's data protection law is largely based on the EU GDPR[20] and tailored through the Data Protection Act 2018.[21] The UK law is based on key principles which include: fair, lawful, and transparent processing; purpose limitation; data minimisation; accuracy, storage limitations; Data security, and accountability.[22] Data Fiduciaries have to ensure that individuals can exercise their rights regarding their personal data, including the rights of access, rectification, erasure, restriction, data portability, objection and those related to automated decision-making.[23] In terms of cross border data flow, the UK prescribes adequacy standards. Section 74(a) and 74(b) of chapter V of the Data Protection Act 2018 provides the adequacy standards for international transfer of data.[24] It requires that the third country must be a privacy-respecting and a rule of law based state, respecting human rights and freedoms. Recently, the UK Secretary of State has laid the international data transfer agreement (IDTA), addendum to the European Commission's standard contractual clauses for international data transfers (Addendum) and a document setting out transitional provisions before the Parliament.[25]

On the non-personal data front, UK data protection law does not cover non-personal data. Similar to the EU, it takes the position that data protection

[19] *European Union (Withdrawal) Act 2018.* (n.d.). GOV.Uk. Retrieved March 21, 2022, from https://www.legislation.gov.uk/ukpga/2018/16/contents/enacted.
[20] *GDPR vs. UK-GDPR; the laws Post Brexit.* (2021, November 4). Lexology. Retrieved March 21, 2022, from https://www.lexology.com/library/detail.aspx?g=430eb8f4-8d52-4229-be9e-bb1b0f74fd56.
[21] *Data Protection Act 2018.* (n.d.). GOV.Uk. Retrieved March 21, 2022, from https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.
[22] Ibid
[23] *Lawful basis for Processing.* (n.d.). Information Commissioner's Office. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/.
[24] *Data Protection Act 2018.* (n.d.). GOV.Uk. Retrieved March 21, 2022, from https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.
[25] *International data transfer agreement and guidance.* (2022, February 2). ICO. Retrieved March 21, 2022, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

principles must only apply to such information concerning an identified or identifiable natural person. The UK makes explicit provisions for the independence of the data protection authority. The Information Commissioner (whose functions are discharged through the ***Information Commissioner's Office ("ICO")*** is the supervisory authority for the UK for the purposes of Article 51[26] of the UK GDPR. Clause 2(2) of schedule 12 states that *"No recommendation may be made to Her Majesty for the appointment of a person as the Commissioner unless the person concerned has been selected on merit on the basis of fair and open competition"*. Clause 5(1) of the same schedule gives power to the Commissioner to appoint such staff as he/she deems fit.

The UK legislation provides for specific cases where such exemptions may be granted under schedules 2, 3 and 4 of the Data Protection Act 2018, wherein certain provisions relating to the data protection act will not be applicable to exempted entities.

2.2. India

India's data protection regime is evolving with continuous efforts to enact a uniform and overarching law. Towards this, three drafts have been placed in the public domain till date. The first set of recommendations was given by the Committee of Experts under the chairmanship of Justice B.N Srikrishna (Retd.), a former judge of the Supreme Court of India. Their report '*A free and fair digital economy, Protecting Privacy and Empowering Indians'*, was the basis of a bill that was introduced to Parliament of India in 2018.[27] Thereafter a subsequent version of the Bill was tabled in the Parliament in 2019, which was sent to a Joint Parliamentary Committee (JPC).[28] After extensive deliberations and recommendations from the committee, another version of the draft with significant changes was produced on 16th December, 2021.[29]

The JPC has proposed an all encompassing legislation which will govern personal as well as non-personal data. The report has made its recommendation based on the economic potential that data offers and identifies data as an 'asset of national importance' and focuses on the need to unify data sets. It is on these parameters that the committee has included non-

[26] *General Data Protection Regulations.* (n.d.). EU Parliament. Retrieved March 21, 2022, from https://www.privacy-regulation.eu/en/article-51-supervisory-authority-GDPR.html.

[27] *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians Committee of Experts under the Chairmanship of Justice B. (2018, July 27).* MeitY. Retrieved March 21, 2022, from https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

[28] *The Personal Data Protection Bill 2019. (2019, December 5).* Retrieved March 21, 2022, from http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[29] *Report of the Joint Committee on the Personal Data Protection Bill, 2019.* (2021, December 16). Lok Sabha. Retrieved March 21, 2022, from http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf.

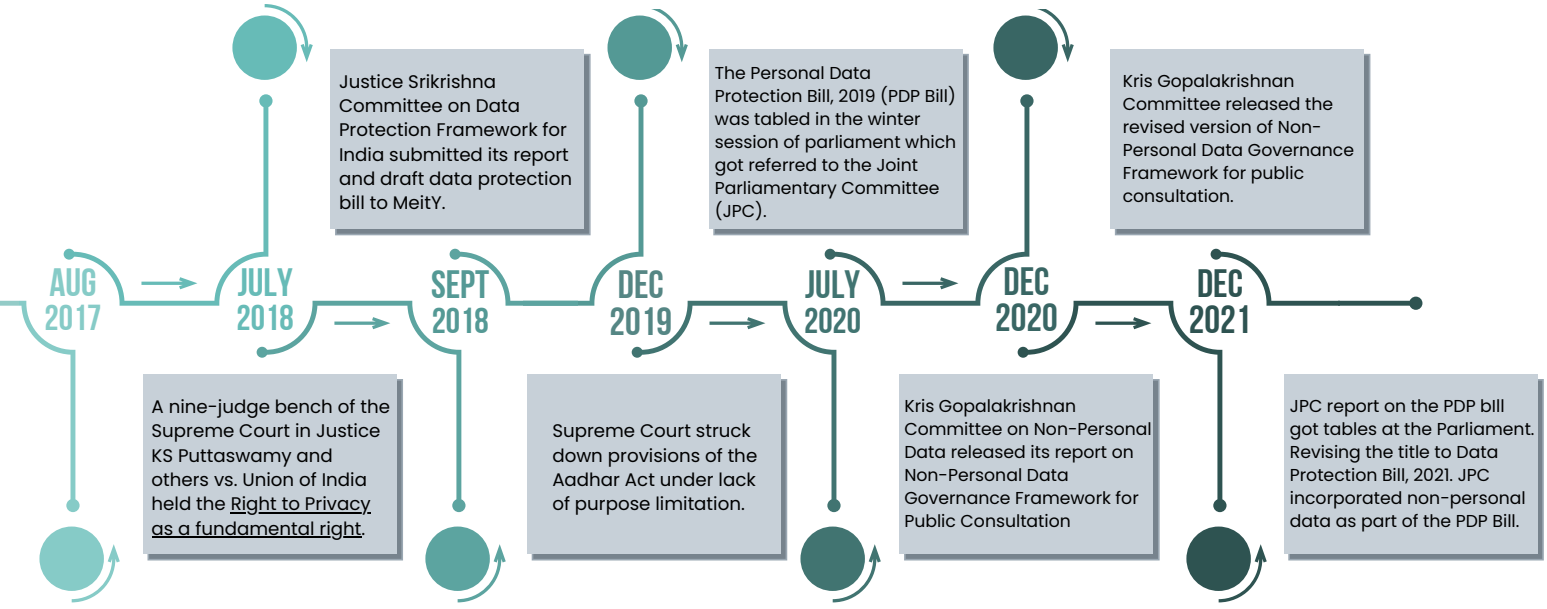

Figure 2: Key milestone in India's data protection journey

personal data in the legislation as well. Clause 2(a) and 2(d) of the draft bill now reads as *"provisions of the act shall apply to (a) processing of the personal data…; (d) the processing of non-personal data including anonymised personal data."* The committee has also defined non-personal data, however, it is the view of the tech ecosystem, as heard in extensive consultations, that the definition is not nuanced to truly bring out the intricacies of non-personal data.[30] It is also worth noting here that a separate committee headed by Kris Gopalakrishnan has already come out with two drafts of non-personal data regulation and has called to approach non-personal data distinct from personal data.[31]

In continuation from the previous version of the Bill, the JPC report retained strict data localisation requirements with an objective to protect national security interests, privacy and generating employment.[32] India's Data Protection Bill requires the mirroring of copies of the sensitive data to be stored in India and restricting the transfer and processing of critical personal data abroad. In fact, non personal data has also been included in the proposed legislation and towards that Clause 92(2) which mandates sharing of non-personal data including anonymised datasets with the government.

[30] Rizvi, K., & Venkatesh, K. (2020, August 31). *Why non-personal data governance framework needs a rethink. The Financial Express.* Retrieved March 21, 2022, from https://www.financialexpress.com/opinion/why-non-personal-data-governance-framework-needs-a-rethink/2069892/; *Submission to the Report by the Expert Committee on Non Personal Data Governance framework.* (n.d.). The Dialogue. Retrieved March 21, 2022, from https://thedialogue.co/wp-content/uploads/2020/09/NPD-Submission-_-The-Dialogue.pdf.

[31] *Report by the Committee of Experts on Non-Personal Data Governance Framework.* (n.d.). Meity. Retrieved March 21, 2022, from https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf.

[32] *Report of the Joint Committee on the Personal Data Protection Bill, 2019.* (2021, December 16). Lok Sabha. Retrieved March 21, 2022, from http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

3. INTEROPERABILITY

Interoperability plays a critical role in the digital ecosystem. Benefits from data are maximised when it is Findable, Accessible, Interoperable and Re-usable.[33] In its Digital Agenda, the EU Commission has identified a lack of interoperability as one out of seven "most significant obstacles" to the "virtuous cycle" of digitalisation.[34] However, while placing importance on interoperability in the digital ecosystem, one must remain aware of how interoperability is a means to achieve better efficiency of a system and it incurs both cost and reaps benefits.

Interoperability in technical terms can be understood in the following two forms:

1. **Horizontal Interoperability:** Wherein competing products, platforms or systems are interoperable.[35] For example, in horizontal interoperability, users of different messaging platforms would be able to communicate with each other directly.
2. **Vertical interoperability:** This refers to the interoperability of a product, service or platform with complementary products and services.[36] For example, in vertical interoperability, a messaging platform could tie up with an e-commerce platform to share their purchases and allow them to make similar purchases.

Interoperability in both these manifestations helps to enhance the effectiveness of data by presenting or storing in standardised models, coupled with easy data transfer protocols to enable knowledge and insight sharing. In the context of data protection, interoperability is a precondition for the interconnectedness and free flow of data that is crucial for a data-based economy, and therefore for data-driven innovation.[37]

The Indian government has been driving interoperability for a long time at the domestic level. In 2015, the Indian government presented interoperability in the e-governance framework[38] where it proposed to achieve goals of data

[33] Thomas, C. (2017). *IPR, Technology Transfer & Open Science. JRC Publications Repository.* Retrieved March 21, 2022, from https://publications.jrc.ec.europa.eu/repository/bitstream/JRC106998/kj1a28661enn.pdf.

[34] *A Digital Agenda for Europe.* (2019, May 19). EU Commission. Retrieved March 21, 2022, from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF.

[35] *Access to, and Interconnection of, Electronic Communications networks and associated facilities (Access Directive) Article 2 lit. (b).* (2002, March 7). European Parliament. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0019&from=EN.

[36] Farrell, J., & Simcoe, T. (2012, August). *Four Paths to Compatibility - Oxford Handbooks*. Oxford Handbooks Online. Retrieved March 21, 2022, from https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780195397840.001.0001/oxfordhb-9780195397840-e-2.

[37] Kerber, W., & Schweitzer, H. (2017). *Interoperability in the Digital Economy*. Journal of Intellectual Property, Information Technology and Electronic Commerce Law. Retrieved March 21, 2022, from https://www.jipitec.eu/issues/jipitec-8-1-2017/4531/JIPITEC_8_1_2017_Kerber_Schweitzer.pdf

[38] *Interoperability Framework for e-Governance (IFEG)*. (2015, October). Ministry of Communications and Information Technology. Retrieved March 21, 2022, from http://egovstandards.gov.in/sites/default/files/Interoperability%20Framework%20For%20e-Governance%20(IFEG)%20Ver.1.0.pdf

exchange through infrastructure and software (technical ability), meaning exchange (ability to comprehend data in the same way as it was provided) and process agreements (ability of organisations to provide services to other organisations or clients). Similar interoperability also needs to be achieved at the international level in terms of data flow.

A regulatory interoperability framework will be to India's benefit in multiple sectors. If one looks at the BPO sector for instance, the benefits of data flow are clear in supporting its growth. Yet, currently, due to the tedious process of Standard Contractual Clauses and Binding Corporate Rules, there are an inordinate amount of delays and bureaucratic hurdles that exist for businesses operating in India. An interoperable regime would help to further growth of this sector.

The National Digital Communications Policy 2018 also ensures interoperability in emergency situations in a network-agnostic, operator-agnostic and technology-agnostic manner.[39] In 2020, the Ministry of Electronics and Information Technology in its white paper on National Open Digital Ecosystem (NODE)[40] presented openness and interoperability as the first principles for the NODE architecture.

Moreover, interoperability helps in driving innovation, competition, accessibility, openness and flexibility and transcends sectors. For example, in the healthcare system, interoperability could play a crucial role in accessing the health records and treating patient illness across jurisdictions.

Countries globally are working to develop and implement data privacy frameworks that can adequately protect data of their citizens, while simultaneously allowing data to flow across borders in ways that support trade and innovation. To realise its ambitions of a world-leading economy, India should therefore look at enacting data sharing frameworks with the EU, US, UK and other major nations, to allow free flow of data across borders while protecting user privacy.

India's data protection standards could be enhanced to bring the country closer to an alignment and harmonisation with international standards and laws on data protection, taking a step forward towards making India eligible and compliant to enter into such frameworks.

[39] *National Digital Communications Policy 2018.* (n.d.). Department of Telecommunications. Retrieved March 21, 2022, from https://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf.

[40] Note: This whitepaper seeks to enable ecosystems that would provide seamless service delivery, and foster innovation through the open sharing of data.

Moreover, for law enforcement agencies from India to access data, the new data protection regime will allow India an opportunity to engage with countries such as the US under the CLOUD Act, which is also based on certain adequacy requirements, such as *"robust substantive and procedural protections for privacy and civil liberties in light of the data collection" and "sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data".*

4. HARMONISING INDO-UK DATA PROTECTION REGIME: ROADBLOCKS

4.1. Adequacy Standards

The UK's international data transfer openness depends on the adequacy standards met by the transferee countries. The Secretary of State has to consider that an *"adequate level of protection to the personal data"* [41] is provided in the country or organisation where data is being transferred. As per Section 74A of the Data Protection Act 2018, three key considerations have been provided before authorising the transfer of the data i.e. *a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation..... including concerning public security, defence, national security and criminal law. b) the existence and effective functioning of one or more independent supervisory authorities. c) the international commitments the third country or international organisation concerned has entered into.*[42]

Further, up until before the Schrems rulings, majority International Data Transfer Agreements were done on the basis of Standard Contractual Clauses signed between the two countries. However, as a result of the Schrems I and II ruling (refer to Box 1), organisations must now carry out a detailed assessment of whether the transferred personal data will be subject to a level of protection that is essentially equivalent to that which it would receive in the UK. This assessment is required for all existing SCCs, and for all new SCCs, including those that will utilise the new International Data Transfer Agreement ('IDTA') proposed by the UK Information Commissioner's Office ('ICO').[43]

Of the three considerations mentioned above, India has:

i. A rich jurisprudence respecting rule of law, human rights and fundamental freedoms and is working to legislate a data protection law after extensive consultation following due Parliamentary checks and procedure.

ii. The proposed data protection law in India seeks to establish an independent data protection authority. The Government of India does however retain certain

[41] *Chapter V - Transfers of Personal Data to Third Countries*. (n.d.). Data Protection Act 2018. Retrieved March 21, 2022, from https://www.legislation.gov.uk/ukpga/2018/12/part/3/chapter/5/enacted.
[42] Ibid.
[43] *International data transfer agreement and guidance*. (2022, February 2). ICO. Retrieved March 21, 2022, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

residuary powers whose exercise may conflict with the independence of the Data Protection Authority (DPA). Any implications of the use of such powers will only be clear once the law is enforced. It would be helpful if the Government reviews the existence of such powers.

iii. In terms of government exemptions envisaged in Clause 35, it is worth appreciating that the DPB, 2021 has included the protections envisaged in the Puttaswamy by way of explanation in Clause 35.

Box 1: Schrems II Judgement

The Privacy Shield framework presents the possibility of lawful transfer of personal data from the EU to the United States, while ensuring a strong set of data protection requirements and safeguards. On the basis of this framework EU (later European Economic Area (EEA)) businesses were able to transfer personal data to US-based companies that were listed in the Privacy Shield list.[44] The CJEU invalidated the EU-US privacy shield agreement and ruled against the use of Standard Contractual Clauses. The court held that:

"As regards judicial protection, the referring court states that EU citizens do not have the same remedies as US citizens in respect of the processing of personal data by the US authorities, since the Fourth Amendment to the Constitution of the United States, which constitutes, in United States law, the most important cause of action available to challenge unlawful surveillance, does not apply to EU citizens. In that regard, the referring court states that there are substantial obstacles in respect of the causes of action open to EU citizens, in particular that of locus standi, which it considers to be excessively difficult to satisfy. Furthermore, according to the findings of the referring court, the NSA's activities based on E.O.12333 are not subject to judicial oversight and are not justiciable. Lastly, the referring court considers that, insofar as, in its view, the Privacy Shield Ombudsperson is not a tribunal within the meaning of Article 47 of the Charter, US law does not afford EU citizens a level of protection essentially equivalent to that guaranteed by the fundamental right enshrined in that article."

[44] *The CJEU Judgement in the Schrems II Case*. (n.d.). European Parliament. Retrieved March 21, 2022, from https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.

4.2. Data Protection Authority

The Data Protection Authority or any supervisory authority is the foundation of the entire data protection regime of the country. As mentioned in section 2.1., the Information Commissioner (whose functions are discharged through the ***Information Commissioner's Office ("ICO")*** is the supervisory authority for the UK for the purposes of Article 51[45] of the UK GDPR. The power to appoint the information commissioner rests with Her majesty and to keep its independence, Clause 2(2) of schedule 12 maintains that *"No recommendation may be made to Her Majesty for the appointment of a person as the Commissioner unless the person concerned has been selected on merit on the basis of fair and open competition".* Clause 5(1) of the same schedule gives power to the commissioner to appoint such staff as he deems fit.

The UK protects the independence of ICO so much so that when the Department of Culture Media and Sports (DCMS), the body under which the ICO operates, had stated it was considering providing the Secretary of State powers to appoint the CEO of ICO, some of these powers include setting up of its objectives and strategic plans - ICO indicated the following response to ensure the importance of independence in the structure and function of the DPA.

"We agree that, in order for the ICO to continue to function independently, particularly in relation to our regulatory interventions, we should be responsible for setting our own operational objectives and strategies (paragraph 344). This would ensure the ICO retains our independence from government in regulatory and organisational decision-making, allowing us to effectively discharge our duties as a UK regulator. This independence is also an important factor in preserving the ICO's international role and ability to influence on behalf of the UK government and its citizens and businesses to enhance trade and support cross border data flows." [46]

Therefore, without such a separate and independent data regulator, India's chance to be considered adequate for the cross border data transfer with the UK may be reduced, impacting India's position in the global digital economy. The EU GDPR, the global forerunner of data governance regulations, specifically mentions the need for a Data Protection Authority established under its requirements to act with complete independence while exercising duties as a prerequisite for adequacy decisions.[47]

[45] *Article 51 - Supervisory Authorities*. (n.d.). General Data Protection Regulations. Retrieved March 21, 2022, from https://www.privacy-regulation.eu/en/article-51-supervisory-authority-GDPR.html.
[46] *Response to DCMS consultation "Data: a new direction"*. (2021, October 6). ICO. Retrieved March 21, 2022, from https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf.
[47] *Art. 45 GDPR – Transfers on the basis of an adequacy decision*. (n.d.). General Data Protection Regulation. Retrieved March 21, 2022, from https://gdpr-info.eu/art-45-gdpr/.

The EU on the other hand believes that accountability works best when it is coupled with effective enforcement, which it views as either one or several sanctions, elements of supervision, and the possibility to intervene by a supervisory authority.

The power to appoint and remove the members of the DPA remains in the hands of the executive. While the JPC report recommends the addition of the Attorney General, Directors of the Indian Institute of Technology (IIT) and the Indian Institute of Management (IIM), and an independent expert appointed by the central government in the selection committee, even these new additions will be appointed by the central government, making the process executive heavy.[48]

4.3. Government Exemptions

India's draft legislation gives blanket exemption to the government agencies from the application of the legislation under section 35 and 36 on account of *"interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order".* This exemption is not qualified by any accountability provision other than reasons for such order to be recorded in writing. Further, it provides 'necessary and expedient' as two key criteria for exempting government agencies as opposed to 'necessary and proportional' which was prescribed in Puttaswamy judgement and Justice B.N Srikrishna committee report. It is pertinent to note that the Supreme Court has specifically outlawed 'expedience' as a standard and mandated 'necessity' in the Rangarajan judgement.[49]

Furthermore, the mandate for the State to follow a procedure which is 'just, fair, reasonable and proportionate' does not fulfil the mandate in the Puttaswamy-1 judgement, as the 'just, fair, reasonable and proportionate' is only a procedural guarantee and not a substantive touchstone for the State to invoke exemption under Clause 35. The State can invoke exception under clause 35 by simply showing necessity or expediency and need not demonstrate the necessity and proportionality as mandated in the Puttaswamy-1 judgement. To ensure actual accountability and check on State power, it is crucial that instances or purposes for which such exemptions may be granted are explicitly laid down.

[48] *Report of the Joint Committee on the Personal Data Protection Bill, 2019*. (2021, December 16). Lok Sabha. Retrieved March 21, 2022, from http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf Clause 42 and 86 (para 2.266 on pg 160).

[49] S. Rangarajan & ors v. P. Jagjivan Ram 1989 SCC (2) 574, retrieved from https://main.sci.gov.in/judgment/judis/7986.pdf.

4.4. Data Localisation

Various studies demonstrate that data localisation may restrict the ability of local companies to compete in the global marketplace by limiting access to the global supply chain. This isolation may result in reduced investment and access to capital and customers. The seamless flow of data across the border is crucial to enable innovation, economic proliferation, and competition which would, in turn, enhance consumer welfare. However, the Government may want to localise data towards access for national security purposes. To that point, the localisation of data should be transparent and based on the minimum necessary procedures to achieve the objectives of national security.

In addition, the free flow of data can particularly help the SME sector and start-ups by expanding and enabling access to the global supply chain. Clause 33 and 34 of the bill presented by JPC places certain restrictions on the transfer of sensitive and critical data outside India specifying strict data localisation requirements. There is a need to find the right approach towards balancing the call for data sovereignty with a non-intrusive method for the companies to transfer data.[50]

International data transfer in the EU is guided by the idea of continuity of protection. There is a notion that data is not stationary and can be moved very easily and therefore protections established at a national level would be incomplete if there are no rules on international data transfers. EU GDPR and the law enforcement directive has a special section to deal with international data transfers. These rules are open to data transfers and don't aim to prevent data transfer but to ensure protection.

In the EU, the most comprehensive method of regulating data transfers is that of an adequacy finding/decision, which is a declaratory document that finds that a third country has a very comparable level of data protection framework in place. Adequacy findings allow third countries to be treated as members of the EU market with respect to data transfers. Aside from this, there are other instruments like contractual tools, protection provisions that commercial operators or public authorities incorporate into commercial agreements entered into between them. This has the main elements or safeguards that are enforceable against third-country parties. The EU also has the ability to sanction certain model clauses in this regard, on that basis of which entities can transfer data to other countries.

[50] Arya T., Karthik V., Trisha P., (January 2021). Impact Study: Personal Data Protection Bill On The Start-Up Ecosystem. New Delhi. The Dialogue, Retrieved From: https://thedialogue.co/wp-content/uploads/2021/01/Startup-Report-Final-Document-vF.pdf?fbclid=IwAR1XJJURqA5EHB_IdBpCxEloTpPlqXbXpzFu8HW7L3R_HwZA1eKDdq2eDo4.

The UK deals with cross border data based on adequacy standards and has similar principles behind it. **Section 74A and 74B of the UK's Data Protection Act 2018** provides the adequacy standards for the international transfer of data. The adequacy standards require that the third country must be a privacy-respecting and a rule of law based state, respecting human rights and freedoms as well as have an independent data protection authority along with right international agreements.

Apart from adequacy, section 75 of the said Act prescribes that data can also be transferred if the third country has appropriate safeguards. These safeguards include a legal instrument in that third country that binds the recipient of transferred personal data to protect such data and an assessment by the controller (data fiduciary) that concludes that appropriate safeguards exist in that country. Further, section 76 also prescribes that in special circumstances (listed out in S. 76), the data can be transferred to a third country. It is important to note here that the regulation does not expressly prohibit data transfer, however, the criteria for transfer of data has been put on a higher pedestal.

A similar approach could be taken in the Indian context as well. Moreover, model contractual clauses and codes of practice could also be a good starting point in finding a balance but there needs to be more clarity on whether DPA would be creating these.

Other best practice mechanisms include:

- The most relevant international transfer mechanisms, aside from an adequacy finding, are contractual clauses and binding corporate rules (BCRs) which are designed to ensure that companies provide a high level of data protection.

- The Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system implements the APEC Privacy Framework and provides a means for self-assessment, compliance review, recognition/acceptance and dispute. It offers baseline protection across different legal regimes, supports certified companies and governments to transfer personal information in a safe and compliant way and enables cooperation between DPAs.

- Participating economies include Australia, Canada, Chinese Taipei, Japan, the Republic of Korea, Mexico, Singapore and the United States of America. Where there are no applicable domestic privacy protection requirements in a country, the CBPR system is intended to provide a minimum level of protection. Unlike the GDPR, which is a directly applicable regulation, the

CBPR system does not displace or change a country's domestic laws and regulations.

Participating companies within these economies are required to develop and implement data privacy policies consistent with 50 programme requirements of the system to a certified CBPR Accountability Agent (public or private sector entity) and to demonstrate that programme requirements will be legally enforceable.

4.4.1. Business Concerns

While there are various considerations to be taken by regulators and legislators behind data localisation, arguably the key considerations of the government behind data localisation include (a) Economic development: To promote domestic innovations and competition in the information technology sector as a large quantum of data is generated within India. (b) Security concerns: To have faster access to data for legal enforcement purposes. While both are legitimate goals and requirements, data localisation may not necessarily help in access to data for law enforcement. Instead, what we need is a data transfer mechanism that reforms the MLAT procedure.

On the contrary, the data localisation mandate (clause 33 & 34 of PDP bill) would increase the compliance burden for businesses in general and those heavily invested in it, with cost implications as they may require changes in the IT infrastructure design to address security issues.[51] It will also have a disproportionate impact on the MSME and start-up ecosystem, raising entry barriers to both the domestic market (compliance) and global market.

4.4.2. Law Enforcement

In terms of legal enforcement, the cumbersome procedure to secure data access during the investigation leads to disproportionate delays. Moreover, placing restrictions on cross border data flows does not automatically guarantee enhanced security and privacy protections of data.[52] Contrary to the assumption that data security is strengthened depending on its location of storage; data security and privacy outcomes are influenced by factors such as effective processes and independent regulators. The law enforcement access to data in the UK has been clearly defined. This access is governed through the six principles in Data Protection Act 2018 i.e. fair, lawful, and transparent processing;

[51] Mehta, S., Venkatesh, K., Shreya, S., Tiwari, P. B., & Malik, S. (n.d.). *Preliminary Analysis: Report Of The Joint Parliamentary Committee On The PDP Bill, 2019.* The Dialogue. Retrieved March 21, 2022, from https://thedialogue.co/wp-content/uploads/2021/12/Final-Preliminary-Analysis-_-JPC-Report-on-PDP-Bill-2019.pdf.

[52] Burman, A., & Sharma, U. (2021, April 14). *How Would Data Localization Benefit India?* Carnegie India. Retrieved March 21, 2022, from https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291.

purpose limitation; data minimisation; accuracy, storage limitations; Data security, and accountability.[53] The processing can only be done for the primary purposes by a competent authority. This primary purpose will define whether the processing is for general purpose or for law enforcement purposes. Data Protection Act 2018 further provides certain rights for the data subject as well as in law enforcement processing. These rights include the right to be informed, right of access, right to rectification, right to erasure etc.[54]

Therefore, it is ideal for India to move towards a less restrictive data localisation regime that provides room for bilateral and multilateral cross-border data transfer agreements and arrangements, for the purpose of helping law enforcement agencies access data, as well as for businesses to participate in the global data ecosystems. It will also be important to have a pan-Government view rather than by sector or by Ministry as it would help in having a uniform approach towards data transfer strategies and approaches.

[53] *Data Protection Act 2018.* (n.d.). UK Parliament. Retrieved March 21, 2022, from https://www.legislation.gov.uk/ukpga/2018/12/part/4/chapter/2/crossheading/the-data-protection-principles.
[54] *Data Protection Act 2018*. (n.d.). UK Parliament. Retrieved March 21, 2022, from https://www.legislation.gov.uk/ukpga/2018/12/part/4/chapter/2/crossheading/the-data-protection-principles (Section 43-48).

5. ROADMAP FOR PROSPECTIVE DATA TRANSFER REGIME

To have effective cross border arrangements, any future FTA between India and the UK must recognise that every stakeholder at both the domestic and international level has a role in legal and regulatory cooperation and coordination. That means establishing cooperation between the FTA enforcement agencies, accountability agencies (data regulators and sectoral regulator), data protection legislation interoperability, other domestic regulatory and legal cooperation (see section 4.2) and international levels (between India and the UK) (see section 4.3).

The UK's current data transfer regime could be made more flexible and practical. The UK has recognised that [55] its crucial to consider viable alternatives to the current standard contractual clauses approach. In this regard, two other transfer tools such as certification schemes and codes of practice could be looked into. Moreover, the report that was published by the Ministry of Digital, Culture, Media and Sports department published in 2021 acknowledges that there might be alternate transfer mechanisms that can be explored to facilitate data transfers internationally. In order to use an alternative transfer mechanism, the UK GDPR requires that the sender must be satisfied that the personal data will be appropriately protected. In practice, the process for organisations using the alternative transfer mechanisms to make an international transfer involves:

- Understanding what data is being transferred, to whom, and to where.
- Identifying an appropriate transfer mechanism.
- Undertaking a risk assessment to ensure that the alternative transfer mechanism provides the necessary protections and that there are enforceable data subject rights and effective redress, accounting for the laws and practices in the recipient country and any supplementary measures which may be required.[56]

5.1. Leveraging Existing Mechanisms to Build towards Interoperability

As it stands, there are a few existing mechanisms that can support the free flow

[55] *Consultation on data: a new direction*. (2021, September 10). GOV.UK. Retrieved March 21, 2022, from https://www.gov.uk/government/consultations/data-a-new-direction.
[56] Ibid.

of data, even with the limited restrictions that are placed on countries through domestic laws. These mechanisms provide avenues for businesses and other stakeholders to make use of the expansion of opportunities for enhanced collaboration.

Market mechanisms

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

- ***Certification schemes***, through which businesses can receive government-recognised third-party data protection certification, which acts as a gate pass for cross-border data transfer.

- ***Codes of conduct***, 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 businesses (within the industry) who had signed the codes. The UK tests these mechanisms as part of its post-Brexit data transfer arrangements.[57]

Binding Corporate Rules (BCR)

This mechanism provides adequate privacy safeguards for making restricted data transfers within the undertaking of businesses, 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 UK GDPR post-Brexit.[58] Both countries can ensure that both data holders and data recipients sign BCR.

Contractual Clauses

Countries use various forms of contractual clause mechanisms. Using this, businesses can participate in restricted cross border data transfer 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.[59, 60] Similarly, the Association of Southeast Asian Nations (ASEAN) has recognised model contractual clauses for data transfers.[61]

[57] 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.

[58] *Binding Corporate Rules.* (n.d.). ICO. Retrieved January 16, 2022, from https://ico.org.uk/for-organisations/binding-corporate-rules/.

[59] 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.

[60] 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.

[61] 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.

5.2. Domestic Coordination

To effect cross border data transfers through an FTA, a concerted effort is needed amongst various actors such as the governments, regulators (specifically the upcoming Data Protection Authority of India), Industry bodies and Civil Society members at the domestic level.

Although there are various bilateral and multilateral transfer mechanisms already being used, the answer might lie in promoting greater interoperability which will require regulators to develop a shared sense of international good practices in data governance through continued sharing of information, knowledge, know-how and ideas on how to tackle these complex issues and developing solutions jointly. It will be important to ensure that approaches are as transparent, non-discriminatory and as least trade-restricting as possible.

Role of Central Government

Currently, in India, data protection regulations are being made under different routes such as legislation, subordinate rules by the executive, and delegated regulation through sectoral regulators and ministries. The enactment of the PDP Bill 2019 (now Data Protection Bill 2021) will bring overarching data protection regulation for India. However, aspects related to domestic harmonisation of various data regulations and coordination of various ministries and sectoral regulators need to be examined.

While in the long run, India is moving towards a uniform data protection regulation, in the short term, the central government (or enforcement agency) must establish high-level coordination amongst the sectoral regulators and policymakers to recognise and implement the cross border data transfer arrangements. Currently, various existing and upcoming regulations contain provisions that require localisation.[62] However, there are also provisions for coordination and harmonisation, that are already built into some of these legislations[63] and policy frameworks[64] [including the PDP Pill 2019[65] (now Data Protection Bill, 2021)]. It could be beneficial for the central government to initiate a conversation on uniform recognition and implementation of the cross border data transfer arrangement utilising these provisions for coordination and harmonisation.

The central government of India could initiate a memorandum of understanding

[62] For instance, the Reserve Bank of India's 2018 circular titled "Storage of Payment System Data" 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.
[63] For instance, Section 21 and 21A of Competition Act, 2002 – coordination between CCI and other statutory authority.
[64] For instance, Chapter 5.3 of Draft Non-Personal Data Governance Framework talks about Harmonisation between NPD regulation and PDP Bill.
[65] Clause 50 (2) & clause 56 – coordination amongst the functioning regulators and governments.

(MoU) with other regulators or authorities governing data for recognising and implementing cross-border data transfer arrangements (through the various tools that are available, including FTAs). To ensure implementation, the MoU must recognise the DPA as the central enforcement authority on cross-border data transfers. The DPA must be empowered to appoint at least one third-party accountability agency to verify compliance of participating businesses with the terms of such transfers between stakeholders. Besides, any dispute resolution related to cross border data transfer must be addressed to DPA, who will coordinate with various coexisting grievance management systems and mandates under different regulations.

In the United Kingdom, the domestic data protection landscape is fairly harmonised, India could pick inferences from UK suitability while harmonising its domestic data protection regulations. The UK adopts parts of the European General Data Protection Regulation (UK GDPR)[66] in its amended Data Protection Act 2018.[67] In addition, the Data Protection Act 2018 also recognises the European version of Privacy and Electronic Communications Regulations (PECR) within its Data Protection landscape. Recognising the overlaps between PECR and Data Protection Act 2018, the ICO suggests these two regulations are complementary in nature, where complying with PECR will aid in complying with Data Protection Act 2018 and vice versa.[68] But the ICO also recommends the data fiduciaries comply with both the regulations to weed out the fall through the cracks.[69] However, to eliminate duplications, Article 95 of UK GDPR[70] (as part of Data Protection Act 2018) exempts network or service providers from UK GDPR (given they comply with PECR) as they have comprehensive provisions within PECR.

In terms of implementation and enforcement, ICO is recognised as the central regulatory authority on data protection matters. Besides, the UK adopts a one-stop-shop approach where ICO has been recognised as an enforcement authority (or "lead supervisory authority") on matters related to cross-border data transfers and processing

Upcoming Regulator Role

While the enactment of PDP Bill 2019 (now Data Protection Bill 2021) will bring overarching data protection regulation for India, concerns related to harmonisation of various data regulations and coordination of various ministries and sectoral regulators remain unaddressed.[71] Our first priority should be to

[66] *The UK GDPR.* (n.d.). ICO. Retrieved March 17, 2022, from https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/.

[67] *Data protection: The Data Protection Act.* (n.d.). GOV.UK. Retrieved March 17, 2022, from https://www.gov.uk/data-protection.

[68] *What are PECR?* (n.d.). ICO. Retrieved March 17, 2022, from https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/.

[69] Ibid.

[70] *Chapter 11 - Article 95 | UK GDPR.* (n.d.). UK GDPR Updated for Brexit. Retrieved March 17, 2022, from https://uk-gdpr.org/chapter-11-article-95/.

[71] Rizvi, K., Towards a progressive Data Protection regime, Times of India, 12 Nov. 2021, Retrieved from: https://timesofindia.indiatimes.com/blogs/voices/towards-a-progressive-data-protection-regime/.

have an Indian regulator be functional at the earliest. Their expertise in the nascent stages of regulation and rulemaking will be critical to creating frameworks that facilitate trade and commerce.

In the short term, it will be beneficial for the Indian Government to engage in high-level coordination amongst the regulators and policymakers, both domestic and foreign, while developing a principle-based framework for data protection. They may hold consultations and dialogues with regulators from foreign jurisdictions on matters that require cooperation such as cross border transfer of data, access for law enforcement and other avenues for coordination.

In the long term, the data protection legislation must provide for systems that facilitate coordination and cooperation between the proposed regulatory authority with other similar authorities in India and outside.

5.3. International Level Coordination and Cooperation

There are various roadblocks in implementing cross border data transfer arrangements between India and the UK which cannot be solved exclusively at the domestic level. A concerted effort is needed from both countries to increase data flow, including through an FTA. While the domestic regulations of India and the UK will differ according to different priorities and domestic constraints, some principles such as privacy by design, transparency and accountability recognised by domestic regulations are congruent. Thus, the objective of the FTA currently being negotiated must be to establish a principle-based cross border data transfer arrangement to build consensus through balancing differences in national constraints and practices while respecting international principles to harmonise data regulation regimes for seamless implementation.

The following must be considered to enhance UK-India cross-border data transfer.

- **Balanced discretion.** While the principle-based approach allows for domestic level discretion in implementation, the flexibility needs to be balanced with the objectives of data transfer arrangements. Moreover, exemptions in the bilateral arrangement for securing national security and

maintaining public order must be narrowly defined and must be less discretionary. At the same time, both countries must lay down fair procedures and scenarios for exemptions in the FTA.

- **Trinity thumb rule.** While India and the UK have various economic and national interests, both 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.

- **Consistency test.** India and the UK should refrain from enacting complicated and disparate future legislation or delegated regulations, which would hamper cross-border data transfers. Therefore, the countries should conduct a consistency test for any future legislation or regulations to check the compatibility with the clauses in the FTA.

- **Choice of Judiciary.** The critical concerns with bilateral agreements such as the FTA are (a) which courts (Indian or UK) should have jurisdiction over specific disputes, and (b) which system of law should govern specific issues (domestic regulations of India or the UK). While it is futile to decide the choice of judiciary or jurisdiction as they may change according to the dispute, it is essential to have guidelines as part of the FTA. Therefore, both the United Kingdom and India must work together to develop guidelines for the choice of judiciary and jurisdiction for potential disputes.

6. CONCLUSION

As this report has made clear, Data Protection law should keep privacy at its core. However, it must also make provisions for data transfer across borders to drive digital trade, foreign direct investment and innovation. It must be noted that the three key considerations, that is, rule of law, independent data authority and international commitments for adequacy standards under UK's DPA, 2018 are made to protect data from misuse and therefore could help enhance data protection in India. Following are some of the recommendation that could help in achieving a data adequacy agreement between the two countries:

- There should be a balance between limiting cross border data flows in the interest of security, against the practicality of such solutions and the political and economic impact such decisions may have.

- The powers of the central government to exempt any government agency from the Act is very wide sweeping and could affect the first consideration taking into account the Schrems II judgement. Exemptions can be granted for processing in the interest of national security, however, must be with adequate safeguards. The GDPR has similar exemptions, however, it has checks and balances that mitigate potential misuse - something the Bill does not seem to address at the moment. Adopting checks and balances can reassure citizens as well as the third country as to the proper access and use of their data by the Government.

- Ensuring a strong and independent Data Protection Authority that is tech-savvy, fairly funded, and works with business will be critical to engendering trust and ensuring the continued relevance of data regulation. It will entrust the citizens as well as meet the adequacy standards.

- NPD regulation is still not established in many jurisdictions and remains nascent. Perhaps the Indian and UK governments could work together, alongside businesses, to develop the most optimum guidelines to encourage both privacy and innovation.

- The UK and India should work closely and collaboratively for a future UK-India Data Adequacy Agreement and a more internationally aligned framework over time. A best practice dialogue between the UK authorities and ICO, with the Indian authorities, should be regular, involving other stakeholders where necessary.

- While India's data protection authority is created, the MeitY can engage with ICO to understand the implementation issues that might be faced by the Indian DPA and once a Data protection bill is enacted and a DPA come into being, both the regulators, namely ICO and DPA, can closely work together on further strengthening the processes.

There should be a continued effort to progress with the evolving digital/data ecosystem. Should these suggestions be followed, we believe that it will be a win-win for the UK and India by enabling digital trade to grow between our countries, supporting innovation and ensuring privacy and security for the masses.

The Dialogue™
INFORM ENGAGE IDEATE

UK INDIA
BUSINESS COUNCIL

Recommended Citation: Tripathi, A., Shekar, K., Venkatesh, K., & Misra-Elder, M. (2022). *Harmonising the UK and India Data Protection Regime.* The Dialogue.

This report analyses the key roadblocks that may come in harmonising the laws of UK and India's data protection law and its relation in improving collaboration between the countries.

https://thedialogue.co

https://ukibc.com