ADDRESSING REGULATORY FRAGMENTATION IN CROSS-BORDER DATA FLOWS

February 2023 | *Issue No. 028*

ESYA centre

Attribution: Vaishnavi Prasad. *Addressing Regulatory Fragmentation in Cross-Border Data Flows*. February 2023, Esya Centre.

Esya Centre
B-40 First Floor
Soami Nagar South,
New Delhi - 110017, India

The Esya Centre is a New Delhi based technology policy think tank. The Centre's mission is to generate empirical research and inform thought leadership to catalyse new policy constructs for the future. More details can be found at www.esyacentre.org.

About the Author: Vaishnavi Prasad is a Research Assistant at the Esya Centre.

Acknowledgements: The author would like to thank Meghna Bal and Mohit Chawdhry for their valuable inputs.

Cover Illustration: Taniya O'Connor

Layout & Design: Khalid Jaleel

CONTENTS

INTRODUCTION

The rules governing cross-border data flows are becoming increasingly fragmented, at the domestic and international level. In April 2020, around 128 of 194 countries had data protection rules in place.[1] While these laws manifest different approaches to cross-border data transfers, trends suggest that restrictions are growing on free data flows. This is exemplified by the number of data localisation measures in force, which has nearly doubled since 2017, with some 144 restrictions in place in 62 countries worldwide.[2]

Further, there are several competing mechanisms governing cross-border data flows. The three main approaches are to use plurilateral arrangements between countries, free trade agreements, or unilateral mechanisms such as data adequacy decisions, model contractual clauses ("**MCCs**"), binding corporate rules ("**BCRs**"), or the Asia-Pacific Economic Cross-Border Privacy Rules ("**APEC CBPR**") Certification. Technology standards and other initiatives by private firms also facilitate cross-border data transfers, but these are outside the scope of this paper.

India assumed the G20 Presidency for the first time on 1 December 2022. [3] The country also published a Digital Personal Data Protection Bill, 2022 around the same time.[4] The draft marks a shift from previous versions, which emphasised data localisation, to an approach that encourages cross-border data flows. India is an important player in global debates on data governance, on account of the quantity of data generated, traded and consumed here.[5]

1. UNCTAD, "Data Protection and Privacy Legislation Worldwide", available at: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

2.Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them", ITIF, available at: https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.

3. G20 Indonesia 2022, "Handover to C20 India-G20 Presidency of Indonesia", G20 Indonesia 2022, available at: https://g20.org/events/handover-to-c20-india/.

4 . Ministry of Electronics and Information Technology, "Digital Personal Data Protection Bill, 2022, available at: https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf

5. Special Correspondent, "At 9.8 GB per month, India has the highest usage per smartphone", available at: https://www.thehindu.com/business/Industry/india-has-highest-data-usage-report/article28078254.ece

In this context, Part I of the paper examines the competing approaches to cross-border data flows and identifies some challenges. Part II explores India's new approach to cross-border data flows, and the opportunity the country can seize to champion a more harmonised regulatory approach.

I. EXISTING MECHANISMS FACILITATING CROSS-BORDER DATA FLOWS

Three mechanisms facilitate transnational flows of data. One, plurilateral arrangements that harmonise the data protection regimes of the signatory countries; two, trade agreements between countries that incorporate provisions facilitating cross-border data flows; and three, unilateral instruments exercised at the country level (such as data adequacy decisions) or between organisations (including model contractual clauses, binding corporate rules, and APEC CBPR certifications).

1. Plurilateral Arrangements

Plurilateral arrangements are international instruments representing a broad consensus between member states on the principles for cross-border data transfers. (Annexure 1) This is usually achieved by aligning the principles that gird the legal frameworks[6] of the signatory states. Such plurilateral arrangements vary in enforceability.

Non-binding arrangements are used to establish broad data protection norms. For instance, the Organization for Economic Co-operation and Development ("**OECD**") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,[7] which harmonise the national privacy legislations of OECD members. Some other non-binding privacy agreements include the ASEAN Framework on Personal Data Protection[8] and the African Union Convention on Cyber Security and Personal Data Protection.[9]

These arrangements exist to encourage the parties to adopt data protection principles. Binding plurilateral agreements, such as the APEC Privacy

6. Casalini, F., J. López González and T. Nemoto, "Mapping commonalities in regulatory approaches to cross-border data transfers", OECD Trade Policy Papers, No. 248, available at: https://doi.org/10.1787/ca9f974e-en.

7. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

8. The ASEAN Framework on Personal Data Protection, available at: https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf

9. African Union Convention on Cyber Security and Personal Data Protection, available at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

Framework and Convention 108+ of the Council of Europe, call on members to provide the requisite privacy protection via domestic law.[10] So far 9 APEC nations of 21 have opted into the APEC Privacy Framework while 55 nations are members of the Modernized Convention 108+.[11]

Some of these agreements have been modernised in response to the rapid evolution of information technology. For instance, Convention 108+ was opened for signature in 1981 as one of the first legally binding international instruments governing data protection. It was modernised in 2018 to include provisions such as transparency, proportionality and accountability, among others.[12] Similarly, the APEC Privacy Framework was initially published in 2005,[13] and updated in 2015.[14]

2. Free Trade Agreements and Digital Economy Agreements

Three main pillars of trade law are the General Agreement on Tariffs and Trade ("**GATT**"), the General Agreement on Trade in Services ("**GATS**"), and the Agreement on the Trade-Related Aspects of Intellectual Property Rights ("**TRIPS**"). While updated a few times in the recent past (such as in the Information Technology Agreement or the working group on e-commerce), WTO law has not evolved adequately to address developments in digital trade.[15] As a result, countries rely on Free Trade Agreements (FTAs) to achieve a degree of certainty in the rules of cross-border data flows. FTAs are treaties between two or more countries designed to reduce barriers to

10. APEC Privacy Framework, available at: https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1#:~:text=The%20APEC%20Privacy%20Framework%20promotes,unnecessary%20barriers%20to%20information%20flows.

11 .Council of Europe Portal, Parties to the Convention 108 in the World, available at: https://www.coe.int/en/web/data-protection/convention108/parties.

12. Council of Europe, "The Modernized Convention 108: Novelties in a Nutshell", available at: https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8.

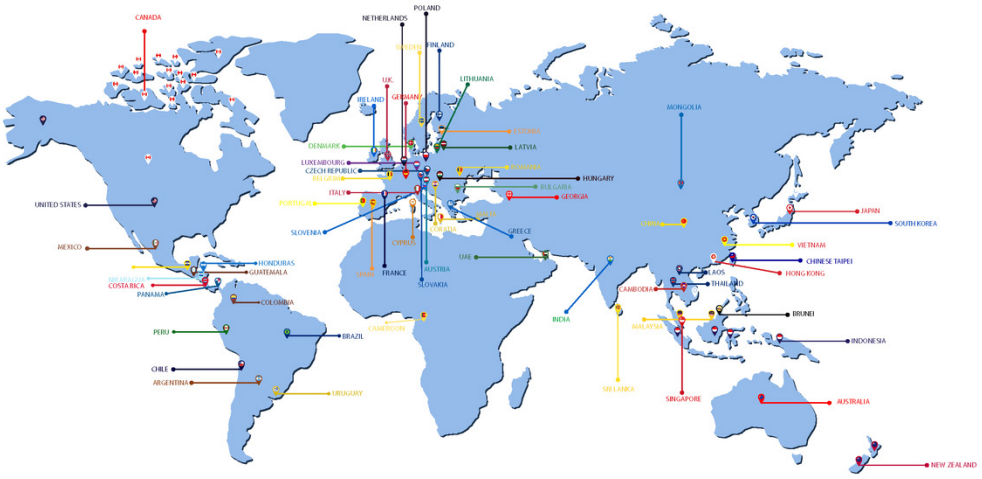
13. APEC Privacy Framework 2005, available at: https://www.apec.org/publications/2005/12/apec-privacy-framework

14. APEC Privacy Framework, 2015, available at: https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

15. See Mira Burri, "The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation", University of California, Davis, available at: https://lawreview.law.ucdavis.edu/issues/51/1/Symposium/51-1_Burri.pdf

trade and investment.[16] Digital economy agreements (DEAs) are specialised agreements that are either subsets of FTAs or standalone agreements facilitating digital trade or e-commerce between countries. Several FTAs and DEAs have provisions facilitating cross-border data flows. These usually require signatories to enact data protection legislation. (Annexure 2).

Figure 1: Countries that have entered into free trade agreements with data transfer clauses



Source: Author's own

Several G20 members have made commitments toward the free flow of data through FTAs. For instance, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership ("**CPTPP**"), the United States-Mexico-Canada Agreement ("**USMCA**"), the US-Japan Digital Trade Agreement, the Singapore-Chile-New Zealand Digital Economy Partnership Agreement, and the Singapore-Australia Digital Economy Agreement.

3. Challenges of Plurilateral Mechanisms and Free Trade Agreements

A. Differing approaches to cross-border data flows contribute to a fragmented international data governance framework

16. Department of Foreign Affairs and Trade, Australia, About Free Trade Agreements, available at: https://www.dfat.gov.au/trade/about-ftas/about-free-trade-agreements.

Many plurilateral agreements contain varying data protection standards and overlapping membership.[17] They also have different default approaches to cross-border data flows. The OECD framework encourages countries not to restrict data flows when there are sufficient safeguards in place.[18] Similarly, the APEC Privacy Framework requires members to ensure that there are no unreasonable restrictions to cross-border data transfers.[19] Conversely, the ASEAN Framework does not explicitly address restrictions on cross-border data flows. And in further contrast, the modernised Convention 108+ is restrictive when it comes to cross-border transfers of personal data. For instance, Convention 108+ deviates from other international agreements like the APEC Framework, as it explicitly lists the circumstances where parties may restrict cross-border data transfers.[20] The inconsistency across frameworks has resulted in a fragmented approach to regulating cross-border data flows.

A fragmented global regulatory framework is disadvantageous for

17 .Casalini, F., J. López González and T. Nemoto, "Mapping commonalities in regulatory approaches to cross-border data transfers", OECD Trade Policy Papers, No. 248, available at: https://doi.org/10.1787/ca9f974e-en.

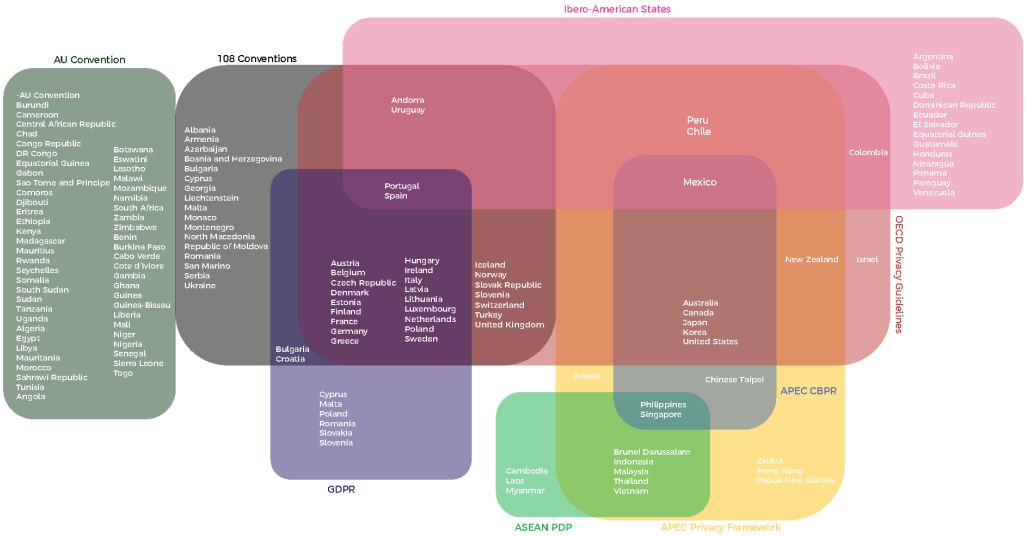
18 . "Article 16: Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure, Article 17: A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation[...]", OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

19 . "Rule 69: A member economy should refrain from restricting cross border flows of personal information between itself and another member economy where (a) the other economy has in place legislative or regulatory instruments that give effect to the Framework or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures (such as the CBPR) put in place by the personal information controller to ensure a continuing level of protection consistent with the Framework and the laws or policies that implement it", https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1)

20 . Article 14: 1. A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may, however, do so if there is a real and serious risk that the transfer to another Party, or from that other Party to a nonParty, would lead to circumventing the provisions of the Convention. A Party may also do so, if bound by harmonised rules of protection shared by States belonging to a regional international organisation, 2. When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to this Convention, the transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Convention is secured, Convention 108+, available at: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf.

business, as it institutes different rights and obligations for the various stakeholders involved, raising the compliance cost for firms. The burden is disproportionately placed on micro, small, and medium enterprises.[21]

Figure 2: The overlapping memberships of plurilateral arrangments



Source: Author's own

As outlined earlier, countries also enter FTAs that facilitate the transfer of personal data. There is a lack of consensus, however, amongst large economies such as the US or China on how to govern cross-border data flows. For instance, the China–Cambodia Free Trade Agreement, though without a provision to explicitly facilitate cross-border data flows, contains a provision that requires each party to maintain domestic laws that protect personal information.[22] Similarly, the China–Mauritius Free Trade Agreement states that each party may take measures it considers "appropriate and necessary" to protect the personal data of users in its jurisdiction.[23] Thus, for transactions that involve processing the data of Chinese citizens, China's Personal Information

21. Nordås, H, "Services Trade Restrictiveness Index (STRI): The Trade Effect of Regulatory Differences", OECD Trade Policy Papers, No. 189, available at: http://dx.doi.org/10.1787/5jlz92022plp-en.

22. Article 10.6, Free Trade Agreement between the Government of the People's Republic of China and the Government of the Kingdom of Cambodia, available at: http://fta.mofcom.gov.cn/cambodia/xieyi/xieyizw_en.pdf

23. Article 11.7, Free Trade Agreement between the Government of the People's Republic of China and the Government of the Republic of Mauritius, available at: http://fta.mofcom.gov.cn/mauritius/annex/mlqs_xdzw_en.pdf

Protection Law ("**PIPL**") would be applicable. The PIPL has provisions to restrict the transfer of personal information to entities outside of China,[24] and it prescribes data localisation in the event that an organisation outside China processes large amounts of personal information generated within the country.[25] In contrast, FTAs anchored by the United States are more likely to contain provisions that explicitly promote the cross-border transfer of data.[26]

B. FTAs may provide differing and inadequate levels of data protection

In their attempts to promote cross-border data flows, FTAs may not mandate strong data protection or use best-effort clauses instead. For instance, in the FTA between the United States and South Korea, Article 15.8 states that it "recognizes the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, the Parties shall endeavour to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders".[27]

Similarly, while the Regional Comprehensive Economic Partnership Agreement has a provision mandating signatories to adopt domestic data protection legislation, it does not specify the extent of data protection necessary. By contrast, the data protection provision of the Singapore Australia Digital Economy Agreement is far more comprehensive. It states that the parties must incorporate specific principles in their data protection framework, such as collection limitation, purpose specifications, and security safeguards among others.[28]

24. Article 41, 42, Personal Information Protection Law, China.

25. Article 40, Personal Information Protection Law, China.

26. Article 11, USA-Japan Free Trade Agreement, available at: https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf; Article 15.8, USA-South Korea Free Trade Agreement, available at: https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file816_12714.pdf; Article 19.11, USMCA, available at:https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf.

27. Article 15.8, US-South Korea Free Trade Agreement, available at: https://ustr.gov/trade-agreements/free-trade-agreements/korus-fta.

28. Article 17, The Singapore-Australia Digital Economy Agreement, available at: https://www.dfat.gov.au/sites/default/files/australia-singapore-digital-economy-agreement.pdf.

Evidently, the standard of data protection offered in FTAs often differs. (Annexure 2) This exacerbates the problem of policy fragmentation and makes it difficult to obtain permission to process foreign data.

4. Unilateral mechanisms

Unilateral mechanisms facilitate the transfer of data to other countries under specified conditions.[29] Normally, a country or organisation applies to the relevant authority for authorisation to receive and process personal data. Often it is the governments or regulatory authorities of the data-exporting country that decide whether the data should be transferred to the importing country.[30] The transfer of data is one-way, hence the mechanism is unilateral. There are four unilateral data transfer mechanisms: model contractual clauses, binding corporate rules, adequacy decisions, and the APEC CBPR certification.

A. Adequacy Decisions

Data adequacy is a statutory prerequisite imposed by a data exporting country upon a data recipient to offer a comparable level of data protection to its own. A data adequacy decision is most often used in the context of the GDPR – which is when the European Commission formally recognises that a non-EU country provides an equivalent level of data protection to the EU under the GDPR.[31] A country with an adequacy decision may receive and process EU data without requiring any further permissions. Any non-EU country that seeks to obtain an adequacy decision enters discussions with the EU. The European Commission is then requested to formally present a proposal to grant adequacy to that country. This is followed by an opinion from the European Data Protection Board, approval from representatives of EU countries, and a final decision by the European Commission.[32] The Commission, while deliberating on whether to grant adequacy, takes into account factors such as the existence of a data protection framework, rule

29. López-González, J., "Trade and cross-border data flows", Going Digital Toolkit Note, No. 11, available at: https://goingdigital.oecd.org/data/toolkitnotes/No11_ToolkitNote_Trade&Data.pdf.

30. For example, the competent Data Protection Authority in the EU approves binding corporate rules, and SCCs and can decide to grant a country an adequacy decision.

31. Article 45, General Data Protection Regulation.

32. European Commission, Adequacy Decisions, available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_e.n

of law, respect for human rights, and the existence and functioning of an independent supervisory authority, among others.[33]

While the concept of data adequacy and a data adequacy decision is most commonly used in the context of the EU, similar provisions that require a third party to have a comparable level of data protection before a transfer can be authorised are in force in several other international data protection frameworks.[34] For instance, Article 14(6) of the African Union Convention on Cyber Security and Personal Data Protection states that data cannot be transferred to a non-African Union member unless they ensure an adequate level of protection of privacy.[35] Similarly, Rule 36 of the Standards for Personal Data Protection for Ibero-American States requires recipient countries to have an appropriate level of protection of personal data by the transferring countries.[36] Countries' own data protection legislations may include adequacy provisions as well. For instance, Brazil's General Data Protection Law requires other countries to provide an adequate level of data protection in order for Brazilian data to be transferred there.[37] Similarly, India's draft Digital Personal Data Protection Bill, 2022 that was recently released for public consultation contains a provision to allow the transfer of personal data to other countries once the Central Government has assessed the factors it considers necessary.[38]

B. Model Contractual Clauses ("MCCs")

MCCs are predetermined contractual terms that may be included in binding legal agreements between a data exporter transferring data to a data importer, which is usually an organisation that operates in another country.[39]

33. European Commission, Working document on Adequacy Referential (wp254rev.01), available at: https://ec.europa.eu/newsroom/article29/items/614108.

34. Article 45, APEC Privacy Framework; Article 6(f), ASEAN Framework on Personal Data Protection; Article 14, Convention 108+.

35. Article 14(6), African Union Convention on Cyber Security and Personal Data Protection.

36. Rule 36, Standards for Personal Data Protection for Ibero-American States.

37. Article 33, Brazilian General Data Protection Law

38. Clause 17, Digital Personal Data Protection Bill, 2022.

39. European Commission, Standard Contractual Clauses, available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en; ASEAN Model Contractual Clauses for Cross Border Data Flows, available at: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.

MCCs prescribe how the data must be treated by the contracting parties. For example, clause 3.10 of the ASEAN MCC for controller-to-processor transfers requires data importers to notify the data exporter if they become aware of any data breach that has affected the personal data in their possession.[40]

Several countries with data protection legislations have published MCCs to facilitate international data transfers.[41] MCCs are also used in international data protection frameworks, and normally have two sets of model contractual clauses: one for data transfers between organisations belonging to member-nations, and the other for transfers from organisations of a member nation to a non-member.[42] Further, there are different templates available based on whether the data transfer is between controllers, processors, or from a controller to a processor.

Sometimes, the use of an MCC must be followed by an evaluation of the quality of data protection offered by the parties involved. For instance, according to the EU General Data Protection Regulation ("**GDPR**"), if data is transferred to a non-European country, the parties to the data transfer agreement containing the Standard Contractual Clauses are required to carry out a transfer impact assessment. A transfer impact assessment documents the specific circumstances of the transfer, the laws in the destination country, and the additional safeguards put in place to protect personal data.[43] In the event of a negative assessment, parties may only transfer data if they incorporate some additional safeguards.

40. Clause 3.10, Module 1: Contractual Provisions for Controller-to-Processor Transfers, in ASEAN Model Contractual Clauses for Cross Border Data Flows, available at: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.

41. Amanda M. Witt and Jon Neiditz, Argentine Data Protection Authority Approves Model Clauses, Kilpatrick Townsend, available at: https://kilpatricktownsend.com/Insights/Alert/2017/1/Argentine-Data-Protection-Authority#:~:text=Argentina's%20Personal%20Data%20Protection%20Law,of%20protection%20for%20personal%20data; Charles Mabbett, Model Contract Clauses for sending personal information overseas, Privacy Commissioner Te Mana Matapono Matatapu, available at: https://www.privacy.org.nz/blog/model-contract-clauses-for-sending-personal-information-overseas/

42. European Commission, Standard Contractual Clauses, available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en; ASEAN Model Contractual Clauses for Cross Border Data Flows, available at: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.

43. Richard Cumbley, Tanguy Van Overstraeten, Georgina Kon, "The Schrems judgement - Transfer Impact Assessments for international data transfers?, available at: https://www.linklaters.com/en/insights/blogs/digilinks/2020/july/the-schrems-judgment.

C. Binding Corporate Rules ("BCRs")

BCRs (also referred to as internal rules, or intra-group schemes) are data protection policies that companies use to transfer personal data within a group of undertakings or enterprises.[44] They ensure that when personal data is transferred across the corporate group, it is in compliance with local laws, and that the data is treated consistently across all relevant entities in the group. BCRs are usually used in the context of the GDPR.[45] Companies submit BCR applications to the relevant data protection authority in the EU, which approves them if they are consistent with the data protection standards of the GDPR.[46]

However, BCRs are not exclusive to the EU and the GDPR. The Association of Southeast Asian Nations ("**ASEAN**")[47] and the Standards for Personal Data Protection for Ibero-American States[48] recognise BCRs as a valid mechanism for regulating data transfers. Similar provisions exist in the data protection laws of several countries such as Australia,[49] Japan,[50] and Singapore.[51]

44. Asian Business Law Institute, "Transferring Personal Data in Asia: A path to legal certainty and regional convergence", available at: https://fpf.org/wp-content/uploads/2021/01/Transferring-Personal-Data-in-Asia-A-Path-To-Legal-Certainty-And-Regional-Convergence-1.pdf

45. Article 47, General Data Protection Regulation; European Commission, Binding Corporate rules, Corporate Rules for Data Transfers within multinational companies, available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en

46. European Commission, Binding Corporate rules, Corporate Rules for Data Transfers within multinational companies, available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en

47. ASEAN Model Contractual Clauses for Cross Border Data Flows, available at: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.

48. Clause 36.1.d, Standards for Personal Data Protection for Ibero-American States.

49. Section 8.1, Australian Privacy Principles; Paragraph 8.21, Australian Privacy Principles Guidelines.

50. Article 24, The Act on the Protection of Personal Information, Japan.

51. Section 26, The Personal Data Protection Act, Singapore.

D. Asia-Pacific Economic Cross-Border Privacy Rules ("APEC CBPR") Certification and Privacy Recognition for Processors ("PRP")

The APEC CBPR Certification is a mechanism to facilitate cross-border data transfers by organisations. It has been likened to BCRs in the EU, but with a broader scope.[52] It can be used for intra-company transfers or transfers to other unaffiliated CBPR-certified companies. The PRP is a companion certification to the CBPR which is applicable for data processors that process data on behalf of controllers.[53] To receive a CBPR/PRP certification, companies must apply to a recognised APEC Accountability Agent, a third-party certification body in an APEC economy. A company can only be certified in the participating APEC economy where it is "primarily located." The Accountability Agent will assess the degree of the company's compliance with the APEC CBPR and provide them with a certification if they are eligible.

The above mechanisms also operate in synchrony at times. For example, the APEC Privacy Framework is a plurilateral arrangement between APEC economies. And the APEC CBPR certification is a unilateral mechanism that implements the APEC privacy framework and draws from its principles. Of the 21 APEC economies, nine have adopted the CBPR system[54] and the rest have made commitments to do so in the foreseeable future. Companies can apply for it and if they receive the certification, they are authorised to process data from participating APEC economies.[55]

5. Challenges of Unilateral Mechanisms

Unilateral instruments for data transfer pose two major challenges to the free flow of data across borders.

52 .Centre for Information Policy Leadership, APEC CBPR & PRP, Questions and Answers, available at: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/cipl_cbpr_and_prp_q_a_final__19_march_2020_.pdf

53 . APEC Privacy Recognition for Processors (PRP) - Purpose and Background, APEC, available at: http://mddb.apec.org/Documents/2015/ECSG/DPS2/15_ecsg_dps2_007.pdf.

54 .APEC, Data Protection in the Asia-Pacific Region and Cross-Border Privacy Rules, available at: http://mddb.apec.org/Documents/2021/CTI/WKSP9/21_cti_wksp9_010.pdf

55 . APEC, "What is the Cross-Border Privacy Rules System, available at: https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system.

A. There is uncertainty in the decision-making process for data adequacy

Data adequacy decisions are usually issued by a data protection authority in one or a group of countries to the recipient country. Since these authorities exercise discretion before authorising the transfer of data, it may sometimes lead to uncertainty in outcomes. The European Commission takes multiple criteria into account in its decisions, including commercial relations, the volume of data flows, the quality of privacy protections offered and also the overall political relationship, the promotion of common values and shared objectives at an international level.[56] This may result in an arbitrary or subjective decision-making process that presents a barrier to the free flow of data.

For instance, the EU has held different countries to different standards. Recently the European Court of Justice invalidated the adequacy decision granted to the United States in Schrems II.[57] The CJEU felt that American public authorities' use of EU data was not restricted by proportionality. However, there have also been several instances where the CJEU found that data collection by British national security agencies also violated EU law.[58] Despite this, the UK was still granted adequacy status.[59]

However, Schrems II points to a larger dissonance between application of the GDPR within the EU and abroad. In EU law, any limitation on the right to privacy for national security purposes must be "necessary and proportionate."[60]

56. European Commission, "Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World", COM/(2017)/7, para 3.1, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN.

57. Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems available at: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:62018CJ0311.

58. Tele2 Sverige AB v. Post-och telestyrelsen, C-203/15 and C-698/15, Court of Justice of the European Union, 2016, available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6819656; Privacy International v. Secretary of State for Foreign and Common wealth Affairs, Case C-623/17, Court of Justice of the European Union, 2020, available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first &part=1&cid=6821354

59. Commission Implementing Decision of 28.06.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, available at: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.

60. Article 52(1), Charter of Fundamental Rights of the European Union; Article 23, GDPR.

Simultaneously, member states have sole responsibility over national security,[61] allowing them the discretion to compromise on data privacy rights – a privilege not given to third countries. Therefore, EU states are effectively exempt from the CJEU standards of necessity and proportionality applicable to others. This results in the European Commission and the CJEU being the sole arbiters of whether any outside country's approach to accessing data for national security purposes is in keeping with the GDPR.

The European Commission released the draft adequacy decision for the EU–US Data Privacy Framework on 13 December, 2022.[62] It remains to be seen whether the decision offers a level of protection that can withstand judicial scrutiny.

B. Other unilateral instruments can pose legal hurdles for micro, small, and medium businesses

Unilateral instruments of data transfer other than adequacy may act as a trade barrier for micro, small and medium enterprises. First, instruments such as pre-approved contractual clauses, Binding Corporate Rules, or APEC CBPR certifications among others, are authorisations that companies must apply for in their own capacity. To do so, they must hire lawyers to obtain authorisation to process personal data, which can be an expensive process. For instance, procuring an SCC still involves a significant cost, estimated at nearly $4000 for micro-businesses, $13,300 for small businesses, $26,000 for medium businesses, and $2,16,000 for large businesses.[63]

Second, small companies are often unaware of SCCs as a means of obtaining data across borders, and are consequently unprepared to set up the same.[64] This asymmetry of information and resources puts them at a disadvantage when negotiating with bigger or more powerful companies for permission to process data. Finally, even if the requisite clauses are in place and permissions are obtained, there is still no guarantee that the company will have access to the data. For instance, after Schrems II, data processors outside the EU are

61. Article 4(2), Treaty of the European Union.

62. European Commission, "Questions & Answers: EU-U.S. Data Privacy Framework, draft adequacy decision, available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_7632

63. New Economics Institute, The Cost of Data Inadequacy, UCL European Institute, available at: https://www.ucl.ac.uk/european-institute/sites/european-institute/files/ucl_nef_data-inadequacy.pdf/.

64. Id.

required to conduct a Transfer Impact Assessment.[65] Therefore, though the validity of SCCs was upheld in Schrems II, there is still uncertainty as the transfers are assessed on a case by case , in the Transfer Impact Assessments. An adequacy decision requires no such additional steps on the part of a company that wishes to process personal data, and this will save smaller firms a considerable amount of resources.

65 .David A. Zetoony, What exactly is a "Transfer Impact Assessment" (TIA), and where the heck did it come from?, The National Law Review, available at: https://www.natlawreview.com/article/what-exactly-transfer-impact-assessment-tia-and-where-heck-did-it-come/.

II. INDIA'S G20 OPPORTUNITY

India's draft Digital Personal Data Protection Bill, 2022 permits the transfer of data across borders after the Central Government has assessed the factors it may consider necessary.[66] Clause 17 of the Bill states: "The Central Government may, after an assessment of such factors as it may consider necessary, notify such countries or territories outside India to which a Data Fiduciary may transfer personal data, in accordance with such terms and conditions as may be specified." However, the Central Government has neither published the factors it deems necessary nor has it specified the terms and conditions of potential cross-border data transfers.

In the draft Bill, the Central Government is to create a list of countries to which companies are allowed to transfer data. However, the Central Government has not yet publicised the criteria it will employ to determine which countries to whitelist. Given that India is presiding over the G20, where data is a consistent theme, it has the opportunity to mainstream a data governance framework that can help harmonise fragmented approaches to the governance of cross-border flows.

(i) What could the whitelisting criteria look like?

The explanatory note to the draft Digital Personal Data Protection Bill, 2022 identifies a list of seven principles that are used as the basis of personal data protection laws in several jurisdictions.[67] They are: (1) lawfulness, fairness, and transparency; (2) purpose limitation; (3) data minimisation; (4) accuracy of personal data; (5) storage limitation; (6) reasonable safeguards against unauthorised collection or processing; and (7) accountability. These principles are affirmed by a study conducted by the OECD on the overlapping principles underlying personal data protection regulations in 56 economies around the world.[68]

66. Clause 17, The Digital Data Protection Bill, 2022.

67. Ministry of Electronics and Information Technology, "Explanatory note to Digital Personal Data Protection Bill, 2022" https://www.meity.gov.in/writereaddata/files/Explanatory%20Note-%20The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf.

68. Casalini, F., J. López González and T. Nemoto (2021), "Mapping commonalities in regulatory approaches to cross-border data transfers", OECD Trade Policy Papers, No. 248, OECD Publishing, Paris, available at: https://doi.org/10.1787/ca9f974e-en.

This includes 18 of 19 G20 nations and the EU.[69] The study reveals that principles such as lawful processing, purpose limitation and transparency have found universal adoption. These principles can act as a basis for 'whitelisting' countries for the transfer of personal data, such as to guarantee that they will offer an equivalent level of protection. (Annexure 3)

(ii) The Central Government must make the criteria for whitelisting countries publicly available

Once the criteria for whitelisting countries are created, they must be publicised. This will promote transparency and ensure the various stakeholders are aware why only certain countries are eligible to process the data of Indian citizens. This is beneficial for several reasons. One, citizens are made aware of the vetting process through which partner countries are evaluated on the level of data protection they offer. Several principles in administrative law, such as the principle of natural justice that requires transparency in the decision-making process, or the principles of fairness and accountability, require public entities to publish the policies they intend to enforce.[70] Two, transparency ensures that any trade with foreign partners is founded on a clear set of expectations from either side. This is likely to remove uncertainty in business. Further, when the whitelisting criteria based on the aforesaid data protection principles are made public, they are less likely to be vulnerable to legal challenge. For instance, when the Schrems II decision invalidated the US–EU Privacy shield, businesses had to navigate an uncertain legal environment.[71] To avoid such a situation, there must not only be transparency in the criteria, they must also adequately protect the privacy

69. The countries considered in the study were: Algeria, Albania, Angola, Andorra, Argentina, Australia, Botswana, Brazil, Canada, Cape Verde, Chile, China, Colombia, Cote d'Ivoire, Ethiopia, European Economic Area (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom + Iceland, Liechtenstein, Norway), Faroe Islands, Ghana, Hong Kong China, India, Indonesia, Israel, Jamaica, Japan, Kazakhstan, Kenya, Korea, Malaysia, Morocco, Mexico, Namibia, New Zealand, Nigeria, Panama, Peru, Philippines, Russia, Serbia, Singapore, South Africa, Switzerland, Taiwan, Tajikistan, Turkey, United States, Uruguay, cited in Annex B, Casalini, F., J. López González and T. Nemoto (2021), "Mapping commonalities in regulatory approaches to cross-border data transfers", OECD Trade Policy Papers, No. 248, OECD Publishing, Paris, available at: https://doi.org/10.1787/ca9f974e-en.

70. M.P. Jain & S.N Jain, Principles of Administrative Law, 9th edition.

71. Theodore Christakis, "After Schrems II : Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe", European Law Blog, available at: https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/

rights of citizens in accordance with the established legal standard.

(iii) Next steps for India at the G20

India assumed the G20 Presidency on 1st December, 2022. This is an ideal time to facilitate discussions on promoting cross-border data flows. These are pertinent in the context of the fragmented and inconsistent global cross-border data transfer landscape. Unilateral instruments often leave cross-border data transfers to the subjective discretion of a regulatory authority. This can be a trade barrier for micro, small, and medium businesses. Plurilateral instruments, on the other hand, have fragmented data protection standards into regional groups and economic blocs. Fragmented, incompatible cross-border data policies pose a risk to the digital economy.[72]

The G20 is composed of some of the world's largest economies that contribute the majority of global data flows,[73] and is well suited to overcome the challenges of fragmentation. It has already attempted to build consensus on the rules for cross-border data flows.[74] Continued attempts at building a global consensus on core principles, guiding values and best practices can be a lodestar for the development of the domestic data protection regime in various countries, via the G20.

As the voice of the Global South, India can champion the needs of developing countries when promoting a mechanism to promote cross-border data flows. India's principles for whitelisting countries should strike a balance between protecting data rights and ease of compliance. While it is needless to emphasise the necessity of data protection, it has been observed that regulations that heavily prioritise data-subject rights often face compliance challenges by businesses. One prominent example is the GDPR, which resulted

72. Asian Trade Centre, "China applies to join DEPA", available at: https://asiantradecentre.org/talkingtrade/china-applies-to-join-depa

73. Krishna Ravi Srinivas, "Shared Understanding and Beyond: Toward a Framework for Data Protection and Cross-Border Data Flows", G20 Insights, available at: https://www.g20-insights.org/policy_briefs/shared-understanding-and-beyond-toward-a-framework-for-data-protection-and-cross-border-data-flows-2/

74.G20 Osaka Leaders' Declaration, available at: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf; G20 Riyadh Leaders Declaration, available at: https://www.mofa.go.jp/files/100117981.pdf; G20 Rome Leaders Declaration, available at: https://www.consilium.europa.eu/media/52732/final-final-g20-rome-declaration.pdf.

in small businesses struggling to navigate the complex legal requirements.[75] Several businesses faced a drastic financial toll while attempting to ensure compliance.[76] Therefore, India's whitelisting criteria must be grounded in clearly defined data protection principles that can easily be made technically implementable. It should endeavour to eliminate ambiguity and reduce compliance costs. India should advocate for such principles at the G20 and attempt to harmonise the fragmented regulations for cross-border data flows at the international level.

75. Helena Webb et. al., "Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation", available at: https://arxiv.org/pdf/1808.07338.pdf

76. Id.

ANNEXURE 1: AGREEMENTS FOR CROSS-BORDER DATA TRANSFERES

Some plurilateral agreements and their prerequisites for cross-border data transfers to member nations.

S. NO.	AGREEMENT	YEAR	PROVI-SION	CRITERIA FOR TRANSFERS
1	OECD Guide-lines on the Pro-tection of Privacy and Transborder Flows of Personal Data	1980 (revised in 2013)	Articles16 and 17	16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure. 17) i. Member countries should refrain from restricting transbor-der flows of personal data unless the recipient country does not observe these guidelines or is likely to circumvent its domestic privacy legislation
2	ASEAN Frame-work on Personal Data Protection	2016	Section 3	The Participants will endeavor to cooperate, promote and implement in their domestic laws and regu-lations the Principles of Personal Data Protection as set out in Para-graph 6 of this Framework (herein referred to as "Principles") while continuing to ensure and facilitate the free flow of information among the ASEAN Member States.
3	African Union Convention on Cyber Security and Personal Data Protection	2014	Article 2	2. Without prejudice to other information obligations defined by extant legislative and regulatory tests in AU member states, state parties shall ensure that any person exercising e-commerce activities shall provide to those for whom the goods and services are meant, easy, direct and uninterrupted access us-ing non-proprietary standards with regard to certain data.

S. NO.	AGREEMENT	YEAR	PROVI-SION	CRITERIA FOR TRANSFERS
4	Modernised Convention for the Protection of Individuals with regard to the processing of personal data	2018	Article 14	A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may, however, do so if there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention. A Party may also do so, if bound by harmonised rules of protection shared by States belonging to a regional international organisation
5	APEC Privacy Framework	2015 (updated from the 2005 Framework)	Paragraph 69	A member economy should refrain from restricting cross border flows of personal information between itself and another member economy where (a) the other economy has in place legislative or regulatory instruments that give effect to the Framework or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures (such as the CBPR) put in place by the personal information controller to ensure a continuing level of protection consistent with the Framework and the laws or policies that implement it.

ANNEXURE 2: FREE TRADE AGREEMENTS PERTAINING TO DATA TRANSFERS

A list of some free trade agreements with provisions pertaining to data transfers.

1. Free Trade: Agreement between the United States of America and Japan concerning Digital Trade ("USA-Japan Digital Trade Agreement")

Provision: Article 15

1. Each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade.

2. Each Party shall publish information on the personal information protections it provides to users of digital trade, including how:

(a) natural persons can pursue remedies; and

(b) an enterprise can comply with any legal requirements.

3. Recognizing that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote interoperability between these different regimes.

4. The Parties recognize the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented.

2. Free Trade: Singapore-Australia Free Trade Agreement, Chapter 14: Digital Economy

Provision: Article 17

1. The Parties recognise the economic and social benefits of protecting the personal information of persons who conduct or engage in electronic transactions and the contribution that this makes to enhancing consumer confidence in electronic commerce.

2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of persons who

conduct or engage in electronic transactions. In the development of its legal framework for the protection of personal information, each Party shall take into account the principles and guidelines of relevant international bodies, such as the APEC Cross-Border Privacy Rules ("CBPR") System and the OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data.

3. To this end, the key principles each Party shall take into account when developing its legal framework include limitation on collection, data quality, purpose specification, use limitation, security safeguards, transparency, individual participation and accountability.

4. Each Party shall adopt non-discriminatory practices in protecting persons who conduct or engage in electronic transactions from personal information protection violations occurring within its jurisdiction.

5. Each Party shall publish information on the personal information protections it provides to persons who conduct or engage in electronic transactions, including how: (a) a natural person can pursue remedies; and (b) business can comply with any legal requirements.

6. Each Party shall encourage enterprises in its territory to publish, including on the Internet, their policies and procedures related to protection of personal information.

7. Recognising that the Parties may take different legal approaches to protecting personal information, each Party shall encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks. To this end, the Parties shall endeavor to exchange information and share experiences on any such mechanisms applied in their jurisdictions and explore ways to promote compatibility between them.

8. The Parties recognise that the CBPR System is a valid mechanism to facilitate cross border information transfers while protecting personal information.

9. The Parties shall endeavor to jointly promote the CBPR System, with the aim to improve awareness of, and participation in, the CBPR System, including by industry.

3. Free Trade: Canada-Peru Free Trade Agreement, Chapter 15

Provision: Article 1508

Recognizing the global nature of electronic commerce, the Parties affirm the importance of: sharing information and experiences on laws, regulations, and programs in the sphere of electronic commerce, including those related to data privacy, consumer confidence, security in electronic communications, authentication, intellectual property rights, and electronic government;

4. Free Trade: United States, Canada, Mexico Free Trade Agreement, Chapter 19, Digital Trade

Provision: Article 19.8

1. The Parties recognize the economic and social benefits of protecting the personal information of users of digital trade and the contribution that this makes to enhancing consumer confidence in digital trade.

2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade. In the development of this legal framework, each Party should take into account principles and guidelines of relevant international bodies, such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013).

3. The Parties recognize that pursuant to paragraph 2, key principles include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability. The Parties also recognize the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented.

4. Each Party shall endeavor to adopt non-discriminatory practices in protecting users of digital trade from personal information protection violations occurring within its jurisdiction.

5. Each Party shall publish information on the personal information protections it provides to users of digital trade, including how: (a) a natural person can pursue a remedy; and (b) an enterprise can comply with legal requirements.

6. Recognizing that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. The Parties shall endeavor to exchange information on the mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them. The Parties recognize that the APEC CrossBorder Privacy Rules system is a valid mechanism to facilitate cross-border information transfers while protecting personal information.

5. Free Trade: Digital Economy Partnership Agreement

Provision: Article 4.2

1. The Parties recognise the economic and social benefits of protecting the personal information of participants in the digital economy and the importance of such protection in enhancing confidence in the digital economy and development of trade.

2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce and digital trade. In the development of its legal framework for the protection of personal information, each Party shall take into account principles and guidelines of relevant international bodies.

3. The Parties recognise that the principles underpinning a robust legal framework for the protection of personal information should include: (a) collection limitation; (b) data quality; (c) purpose specification; (d) use limitation; (e) security safeguards; (f) transparency; (g) individual participation; and (h) accountability.

4. Each Party shall adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction.

5. Each Party shall publish information on the personal information protections it provides to users of electronic commerce, including how: (a) individuals can pursue remedies; and (b) businesses can comply with any legal requirements.

6. Recognising that the Parties may take different legal approaches to protecting personal information, each Party shall pursue the development

of mechanisms to promote compatibility and interoperability between their different regimes for protecting personal information. These mechanisms may include: (a) the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement; (b) broader international frameworks; (c) where practicable, appropriate recognition of comparable protection afforded by their respective legal frameworks' national trustmark or certification frameworks; or (d) other avenues of transfer of personal information between the Parties.

7. The Parties shall exchange information on how the mechanisms in paragraph 6 are applied in their respective jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility and interoperability between them.

8. The Parties shall encourage adoption of data protection trustmarks by businesses that would help verify conformance to personal data protection standards and best practices.

9. The Parties shall exchange information on and share experiences on the use of data protection trustmarks.

10. The Parties shall endeavor to mutually recognise the other Parties' data protection trustmarks as a valid mechanism to facilitate cross-border information transfers while protecting personal information

6. Free Trade: China-Mauritius Free Trade Agreement

Provision: Article 11.7

1. Notwithstanding the differences in existing systems for personal information/data protection in the territories of the Parties, the Parties shall take such measures as they consider appropriate and necessary to protect the personal information /data of users of electronic commerce.

2. In the development of data protection standards, the Parties shall, to the extent possible, take into account international standards and the criteria of relevant international organisations.

7. Free Trade: China-South Korea Free Trade Agreement

Provision: Article 13.5

Recognizing the importance of protecting personal information in electronic commerce, each Party shall adopt or maintain measures which ensure the protection of the personal information of the users of electronic commerce and share information and experience on the protection of personal information in electronic commerce.

ANNEXURE 3: COMMON PRINCIPLES IN DATA PROTECTION LAWS ACROSS THE WORLD

S. NO.	PRINCIPLE	EXPLANATION
1	Purpose limitation	The purpose for which data is collected must be clearly defined. Data collected for a specific purpose may not be used for a new, incompatible purpose.
2	Lawful basis for processing	The data processor is required to state why they're collecting the personal data and must not acquire it through deceit. Data must be processed for a specific and legitimate purpose.
3	Data accuracy	The data processed must be accurate and the processor must not collect more data than necessary for the specified purpose.
4	Storage limitation	Personal data may not be stored indefinitely and must be erased by the data processor after a defined period of time.
5	Data security	The data processor must ensure that the data is protected from unauthorised processing, loss, destruction or damage.
6	Transparency	Data subjects must be informed of what data of theirs is being used and for what purpose, regardless of whether it is collected directly or indirectly as soon as it is collected.
7	Notification/consent in data collection	The data subject must be notified that their data is being collected and their consent must be obtained for the same.
8	Right to access and rectification	Data subjects must have the right to access their personal data, and correct any inaccuracies.
9	Breach notification	Data subjects must be notified if the security of their personal data has been compromised by a breach.
10	Existence of a supervisory authority	There must be an independent supervisory authority to enforce the data protection law, conduct investigations into possible violations, and impose sanctions on entities that violate the law.
11	Sensitive data: Additional measures	Additional measures must be undertaken to protect sensitive personal data. This can be in the form of establishing specific conditions that must be met before sensitive data is processed.

B-40 First Floor
Soami Nagar South
New Delhi - 110017
contact@esyacentre.org
www.esyacentre.org