Published on 2 June 2025

CROSS-BORDER DATA FLOWS IN THE DIGITAL ECONOMY

[2025] SAL Prac 14

Since the advent of e-commerce, digital trade has relied on cross-border transfers of data. Today's digital economy is heavily dependent on cross-border data transfers. This article explains the importance of cross-border data flows and examines the measures that international trade negotiators have taken to secure the free flow of data. Just as the technologies that we rely on for digital transactions have advanced, so too have the policy and regulatory measures that support cross-border data transfers. New versions of these measures have emerged as digital trade agreements ("DTAs") are signed to supplement free trade agreements. This article uses the Digital Economy Partnership Agreement to illustrate how DTAs have developed to support innovative transfer mechanisms and examines some of these new developments that aim to promote convergence and interoperability.

YEONG Zee Kin[1]
LLB (Singapore), LLM (London);
Advocate and Solicitor (Singapore); Solicitor (England and Wales)
Chief Executive, Singapore Academy of Law.

1 The digital economy is an amorphous and evolving term.[2] Fundamentally, it is the integration of information and communications technology to transform businesses. It goes beyond merely digitising some aspects of business activities.

1 This article is based on a speech delivered at the Zhongguancun Forum on 27 March 2025 in Beijing, China. The author wishes to thank Catherine Shen for her helpful comments on an earlier draft of this article.

2 See, for example, Kinza Yasar & Mary K Pratt, "Digital Economy", *Informa TechTarget* <https://www.techtarget.com/searchcio/definition/digital-economy> (accessed 7 May 2025); "What is the Digital Economy?", *Wharton Online* <https://online.wharton.upenn.edu/blog/what-is-the-digital-economy/> (accessed 8 May 2025).

True digitalisation requires deep integration of information and communications technology to re-engineer business processes, often giving birth to new business models. Oftentimes, such digital transformation takes place incrementally, as illustrated by the evolution of e-commerce.

2 E-commerce has been with us since the dawn of the Internet age. It is a story about the digitisation of retail. Book, music and video stores were disintermediated when publishers became able to sell books, audio CDs and movie DVDs through online marketplaces.[3] While e-commerce disrupted traditional retail, only part of a sale transaction moved online, *viz*, the figurative shopping basket and payment. Items still have to be physically shipped from warehouses and delivered to the buyer's doorstep. It cannot be gainsaid that massive changes were wrought in the operations of logistics companies as they are now delivering many smaller packages directly to more buyers, slowly eclipsing their traditional mode of delivering larger cartons to fewer shopping centres or retail shops. They needed to transform warehousing and last-mile delivery operations to support this exponential increase in destinations and packages.

3 As broadband communications technology and mobile computing devices became more prevalent, the digitalisation of retail deepened. It is not just the *sale* of books, music and video that takes place online. Consumption is now decidedly digital as well: we read on our ebook readers, listen to music on our mobile phones and watch movies on our smart TVs. The entire business-to-consumer ("B2C") relationship has become fully digital, with practically no physical touchpoints. New business models that have developed have also changed the texture of the B2C relationship. We are no longer confined to purchasing individual books, music compilations or movies (although we can still choose to). We have the additional option of

3 Strictly speaking, this is not disintermediation in the strict sense but the replacement of brick-and-mortar intermediaries with online intermediaries. The author explores this in greater detail in Yeong Zee Kin, *Technology Regulation in the Digital Economy* (Academy Publishing, 2023) ch 4 and *Law and Technology in Singapore* (Simon Chesterman eds) (Academy Publishing, 2nd Ed, 2025) ch 5.

subscribing to services for ebooks (*eg*, Kindle Unlimited), music (*eg*, Spotify or NetEase Music) and movies (*eg*, Netflix or iQIYI). Businesses desire longer-term relationships with customers, not least because they are also keen to gain deeper insights into consumption patterns and preferences to an extent that was not possible when customers were reading books, listening to CDs and watching DVDs away from their platforms.

4 The digitalisation of retail and the evolution of e-commerce as we transition to a digital economy provide us with a simple example – which some may say is overly simplified – of the digital transformation that is associated with the digital economy. Nonetheless, it sets the stage for our discussion about the role of data and the importance of data flows.

I. Importance of data flows in the digital economy

5 In more traditional e-commerce transactions, purchase and payment take place online but physical delivery is still very much necessary. The information transferred electronically when a customer makes an online purchase is fairly insubstantial in volume, *ie*, identity of the customer, billing and delivery addresses, and payment details. The preponderance of information by volume is contained in the book, music CD or movie DVD that is purchased by and delivered to the customer. With digital delivery of ebooks, music tracks and movies, the volume of data flowing electronically between businesses and consumers is exponentially higher. It can be said that such retail activities are now comprised entirely of data flows.

6 The flow of data has also become bidirectional: as customers consume the content that has been pushed to them, behavioural data, consumption patterns and user ratings are collected by service providers. What is true for books, songs and movies is also true of software: productivity software, games and mobile apps predominately adopt a software-as-a-service ("SaaS") model. As more businesses adopt subscription-based SaaS models, the volume of bidirectional data flows increases as consumption of the services increases. With access to more usage data, businesses apply behavioural analytics to enhance

service delivery, improve customer experience and provide personalised recommendations.

II. Emergence of threats to data flows

7 Unfortunately, not all businesses and end users are able to access the digital economy with equal ease or participate in it to the same degree. Data localisation policies that have emerged in a number of jurisdictions raise regulatory barriers for entry into their markets. Data localisation policies have been justified on a variety of grounds, such as ease of access by law enforcement, regulatory or judicial authorities; or protection of national security, economic stability and social order. Mandating the establishment or use of local computing facilities may put local businesses and end users at a disadvantage. Local computing facilities may not be the best in class or sized for optimal cost effectiveness; local businesses and end users may be denied early access to the latest processing capabilities and have to wait for the technology to cascade to their region. A survey of jurisdictions globally distils four data localisation archetypes, which may exist singly or in combination. The following examples are culled from jurisdictions in South Asia and Southeast Asia:[4]

(a) **Export prohibition** is the most restrictive data localisation measure and is usually justified on grounds of national security or economic stability. For example, public sector data must be stored locally in Indonesia;[5] Vietnam requires all domestic enterprises to store and process their personal data locally;[6] and India requires securities intermediaries and institutions to store and process data locally.[7]

4 The author discuses data localisation trends, covering the Asia Pacific in greater detail in Yeong Zee Kin, *Technology Regulation in the Digital Economy* (Academy Publishing, 2023) ch 5 and *Law and Technology in Singapore* (Simon Chester eds) (Academy Publishing, 2nd Ed, 2025) ch 4.

5 Government Regulation No 71 of 2019 regarding Operation of Electronic System and Transactions.

6 Decree No 53/2022/ND-CP.

7 Securities and Exchange Board of India, *Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)* (Circular No SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033, 6 March 2023).

(b) **Repatriation** is a compromise that recognises that some processing and analyses need to take place overseas but requires that the processed data and insights be repatriated within a fixed period. This measure is slightly less restrictive than export prohibition as it permits temporary offshore processing. For example, payment transaction data may be processed overseas but must thereafter be repatriated back to India.[8]

(c) **Local storage** requirements do not prohibit exports but require a copy – sometimes the primary copy – of the data to be stored locally for easier access by law enforcement, regulatory and judicial authorities. This is sometimes referred to as mirroring.[9] In India, for example, the original copy of foreign investors' data must be stored locally.[10]

(d) The requirement to obtain **regulatory approval** ostensibly provides opportunities for risk assessment and de-risking before data is exported, *eg*, offshore processing of financial data in Indonesia.[11] A variation of this requirement is the submission of impact assessments within a prescribed period after export, with the risk that the export may be invalidated if the risk assessment is found wanting, *eg*, in Vietnam.[12] The risk presented by this measure is that opaqueness of regulatory decisions may lend weight to accusations of arbitrariness and be seen as disguised barriers to trade.

8 Reserve Bank of India, "FAQs – Storage of Payment System Data" <https://www.rbi.org.in/commonman/english/Scripts/FAQs.aspx?Id=2995>at Questions 5 and 6 (accessed 7 May 2025).

9 Though not strictly in the technical sense which means that both copies are identical.

10 Securities and Exchange Board of India, *Framework for Adoption of Cloud Services by SEBI Regulated Entities (REs)* (Circular No SEBI/HO/ITD/ITD_VAPT/P/CIR/2023/033, 6 March 2023).

11 OJK Regulation (POJK) No. 11/POJK.03/2022 regarding the Implementation of Information Technology by Commercial Banks.

12 Decree No 13/2023/ND-CP.

III. Digital trade agreements secure different types of data flows

8 The emergence of threats to global data flows has not escaped the notice of international trade negotiators. They have accordingly developed principles to safeguard cross-border data transfers in the digital economy as free trade agreements ("FTAs") are updated with their digital twins.

9 FTAs reflected the state of e-commerce at the time they were concluded: there were relatively few articles in FTAs that dealt with data and significantly more articles dealing with tariffs for imports. However, almost all FTAs dealt with the *protection of personal data* since international trade negotiators knew that e-commerce relied on transfers of personal data (*eg*, identity information, payment details, billing and delivery addresses) and e-commerce businesses were already adopting behavioural analytics for service improvement and personalisation. FTA signatories agreed to implement domestic laws and measures to protect personal data.

10 Digital trade agreements have emerged to supplement FTAs.[13] They contain significantly more articles that deal with data, such as digital identity, e-invoicing and e-payments, and cross-border data transfers. Additionally, articles on personal data protection are strengthened. As more economies adopted domestic data protection laws, new obligations to foster interoperability had to be introduced, such as recognition of regulatory outcomes and national certification systems, and development of new transfer mechanisms. The approach taken in digital trade agreements has been fairly similar with largely uniform drafting. For the present discussion, the Digital Economy

13 United States-Japan Digital Trade Agreement (7 October 2019) (entered into force 1 January 2020), Australia-Singapore Digital Economy Agreement (6 August 2020) (entered into force 8 December 2020), United Kingdom-Japan Comprehensive Economic Partnership Agreement (23 October 2020) (entered into force 1 January 2021), United Kingdom-Singapore Digital Economy Agreement (25 February 2022) (entered into force 14 June 2022), Korea-Singapore Digital Partnership Agreement (21 November 2022) (entered into force 14 January 2023), EU-Singapore Digital Trade Agreement (7 May 2025).

Partnership Agreement[14] ("DEPA") will be used as it is a multi-lateral digital trade agreement.

(a) **Purchase.** Establishing the identity of buyer and seller is a key step – if not a pre-condition – in the B2C relationship. "On the Internet, nobody knows that you are a dog" is a famous meme that has been with us since the dawn of the Internet age. As e-commerce gravitates towards a subscription-based model in the digital economy, identity verification against external, trusted sources takes on greater importance: the B2C relationship is no longer transactional; it lasts longer with more interactions and is entirely digital. The focus of the DEPA digital identities article[15] is to foster interoperability of national digital identity frameworks and solutions and to that end, knowledge transfer and development of international standards that facilitate interoperability.

(b) **Payments.** Payment transactions begin with a request for payment (*ie*, invoice) and ends with a tender of payment (*ie*, receipt). The DEPA paperless trading module contains articles relating to electronic invoicing and electronic payments.[16] The main thrust of these articles is the development and adoption of international standards that promote interoperability. For e-payments, there is also a commitment to promote the use of Application Programming Interfaces (APIs) and to interlink national e-payment networks.

(c) **Service delivery.** Online services can be delivered to and consumed by customers situated anywhere in the world. Just as global logistics developed to fulfil orders by delivering items – and sometimes limiting the items available to customers – from the nearest warehouse,

14 6 November 2020 (entered into force 28 December 2020), signed by founding members Chile, New Zealand and Singapore; Republic of South Korea acceded on 3 May 2024.

15 Digital Economy Partnership Agreement (6 November 2020) (entered into force 28 December 2020) Art 7.1.

16 Digital Economy Partnership Agreement (6 November 2020) (entered into force 28 December 2020) Arts 2.5 (Electronic Invoices) and 2.7 (Electronic Payments).

so too the delivery of online content. Content Delivery Networks ("CDNs") mirror the global distribution of Tiers 1 and 2 Internet Service Providers (ISPs): they are sometimes located at the same data centres and peer at the same Internet exchanges. Content is streamed to customers from CDNs closest to them for greater network efficiency and reduced latency, making for a better user experience. However, CDNs are not necessarily located in the same country as the customers that they serve. The data module in the DEPA establishes default rules that enable cross-border data transfers.[17]

IV. Principles for cross-border data flows under DEPA

11 In order to safeguard the cross-border flow of data that is central to the digital economy, international trade negotiators have agreed on a set of principles that entrenches the free flow of data across borders as a default rule, while accommodating the possibility that there may be exigencies that warrant limited deviations from this default position. In gist, the data articles under the DEPA establish that:

(a) cross-border transfer of data should be permitted for the conduct of business;[18] and

(b) requirements to locate data storage and processing facilities within the country as a condition for conducting business should be prohibited.[19]

12 The DEPA recognises that there are exceptional circumstances that require some degree of restrictions, namely where there are legitimate public policy objectives ("LPPO") to be achieved. However, restrictions must be necessary, proportionate, fair and non-discriminatory. What this means first is that restrictions must be minimised and may only be

17 Digital Economy Partnership Agreement (6 November 2020) (entered into force 28 December 2020) Module 4 Data Issues.
18 Digital Economy Partnership Agreement (6 November 2020) (entered into force 28 December 2020) Art 4.3.
19 Digital Economy Partnership Agreement (6 November 2020) (entered into force 28 December 2020) Art 4.4.

introduced if they are necessary for achieving an identified LPPO. Having crossed this initial threshold, measures that restrict cross-border data transfers must be further calibrated to ensure proportionality of the restrictions to the level of risk and sensitivity of that data associated with the identified LPPO.

13 Moreover, the restrictive measures must be fair and non-discriminatory. There are two dimensions to this. First, the measures must treat businesses and end users of a similar class in like manner: this is the objective dimension. Second, the application of the measures to a specific case must not be arbitrary: this is the subjective dimension. The requirement of fairness and non-discrimination is not surprising since the object and intent of the DEPA is to facilitate cross-border e-commerce and to remove barriers to trade, even those that are disguised. While transparency is not explicitly stated as a principle, it is an enabler without which it will be difficult to demonstrate both objective fairness by providing access to the implementing laws and regulations, as well as subjective fairness by providing reasons for decisions to show that they are not made arbitrarily.

14 These principles are observed by DEPA signatories and economies that have signed digital trade agreements, none of whom has incompatible national data localisation policies.[20]

---

20 The US White House executive order *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern* (Executive Order 16117 of 28 February 2024) illustrates how restrictions are calibrated to be proportionate to the identified national security risk: restrictions are imposed on limited destination countries, identified categories of data and specified transactions. The US Department of Justice issued a final rule (90 FR 1636) (8 January 2025) designating China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela as countries of concern that pose significant risk of exploiting bulk US sensitive personal and government-related data. The transfers of six categories of sensitive personal data (*ie*, certain covered personal identifiers; precise geolocation data; biometric identifiers; human genomic, epigenomic, proteomic, and transcriptomic data; personal health data; and personal financial data) exceeding certain bulk volumes are either prohibited (*ie*, data brokerage and transactions involving human 'omic data) or restricted (*viz*, transfers under vendor, employment and investment agreements are permitted if they meet prescribed security requirements). See executive order *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern* (Executive Order 14117 of February 28, 2024)<https://www.federalregister.gov/d/2024-04573>
(cont'd on the next page)

V. Ensuring exported personal data is protected to equivalent standard

15 If there is one area that the DEPA contemplates restrictions for, it is the cross-border transfer of *personal* data. The DEPA provides a good example of how restrictions are calibrated, and how transfer mechanisms have developed to facilitate cross-border data flows. There is global consensus that exported personal data needs to be protected to an equivalent standard by the recipient of the data. This can be traced to the Organisation for Economic Co-operation and Development) ("OECD") Privacy Principles, which is in fact entitled *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. The title in and of itself encapsulates the essence that the Privacy Principles are meant to facilitate transborder data flows. It articulates a set of data protection principles that has become a benchmark for equivalence. Indeed, the OECD Privacy Principles exhorts adherents to refrain from restricting transborder flows of personal data between countries that observe these principles.[21] If the recipient operates in a country that does not, then the obligation for the transferor is to ensure that sufficient safeguards exist: disrupting the cross-border transfer of data is not contemplated under the principles.

16 However, not all countries have comprehensive personal data protection laws: some countries rely on sectoral regulations. Despite differences in legal approaches, the global norm is for data exporters to adopt legally binding measures to ensure that recipients provide comparable levels of protection for exported data. This is a common feature of personal data protection laws worldwide. The requirement for equivalent protection in the face

(accessed 7 May 2025), final rule Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons 28 CFR (US) Part 202 <https://www.federalregister.gov/d/2024-31486> (accessed 7 May 2025) and *Fact Sheet: Justice Department Issues Final Rule to Address Urgent National Security Risks Posed by Access to U.S. Sensitive Personal and Government-Related Data from Countries of Concern and Covered Persons* <https://www.justice.gov/archives/opa/media/1382526/dl> (accessed 7 May 2025).

21 OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD/LEGAL/0188) Art 17; see also n 36 below.

of a diversity of legal approaches for regulating personal data has not restricted cross-border data flows but has fomented a variety of legally binding transfer mechanisms, such as consent, contracts and certifications.

17 The DEPA also recognises that different legal approaches may be adopted by different signatories. It fosters convergence of legal frameworks by, first, establishing common data protection principles, though these are implemented in domestic legal systems;[22] and second, promoting interoperability through the development of new transfer mechanisms.[23]

A. Contracts

18 Assessment of equivalence can be challenging for businesses. Recognising these challenges, data protection authorities have developed a library of transfer mechanisms. The most commonly used transfer mechanism is the standard or model contractual clauses. These contractual templates provide a ready solution that most businesses can easily use, with or without modifications. They are designed for business-to-business transactional relationships that are fairly short-term (although they can also be used in longer-term business process outsourcing agreements). Examples include the Standard Contractual Clauses of the European Union ("EU SCCs"), the Model Contractual Clauses of the Association of Southeast Asian Nations ("ASEAN MCCs"), and the Cyberspace Administration of China's Standard Contractual Clauses. While the promulgation of contractual clauses is not new, the *mapping* of such model clauses – such as between the EU SCCs and ASEAN MCCs, and the Ibero-American Data Protection Network's Model Contractual Clauses and ASEAN MCCs – is a development that promotes interoperability by identifying areas of similarities to reduce

22 Namely, (a) collection limitation; (b) data quality; (c) purpose specification; (d) use limitation; (e) security safeguards; (f) transparency; (g) individual participation; and (h) accountability: Digital Economy Partnership Agreement (6 November 2020) (entered into force 28 December 2020) Art 4.2.3.

23 Digital Economy Partnership Agreement (6 November 2020) (entered into force 28 December 2020) Art 4.2.6.

compliance hurdles. This is an example of policy innovation that promotes interoperability.[24]

19 The flexibility of contracts and their potential as an innovative interoperability measure are demonstrated by another example. The Standard Contract for Cross-Boundary Flow of Personal Information Within the Guangdong-Hong Kong-Macao Greater Bay Area, which enables entities operating within China's Greater Bay Area to share data *inter se* (but not export beyond the Greater Bay Area).[25] Businesses operating in the Greater Bay Area that use this standard contract enjoy some benefits. For example, volume restrictions on export under Chinese data laws are lifted. Furthermore, the requirements concerning data protection impact assessment ("DPIA") are reduced: the DPIA needs to cover fewer areas and need not be filed.[26]

20 Oftentimes, groups of companies centralise functions that are performed by specific members of the group, *eg*, human resource, finance, information technology (IT) and research and development (R&D). Intra-group agreements can be used to establish the respective roles and responsibilities within a group of companies. A variation of this is the binding corporate rules ("BCRs"), which achieve the same effect through legally binding corporate governance policies applied uniformly within

24 *Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses* (updated 31 January 2024) and *Joint Guide to ASEAN MCCs and RIPD MCCs* (2025).

25 Macau is not included for the time being. The standard contract is not intended for use by entities that are owners or operators of critical information infrastructure.

26 The areas that the data protection impact assessment ("DPIA") must cover under the Standard Contract for Cross-Boundary Flow of Personal Information Within the Guangdong-Hong Kong-Macao Greater Bay Area ("GBA SCC") are reduced to three from six as required under China's Standard Contractual Clauses. While the DPIA of the GBA SCCs need not be filed, the standard contract proper needs to be filed within ten days of taking effect. See *Implementation Guidelines on the Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong)* Art 8; see also, "Facilitation Measure of 'Standard Contract for the Cross-boundary Flow of Personal Information within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong)'", *Digital Policy Office* <https://www.digitalpolicy.gov.hk/en/our_work/digital_infrastructure/mainland/gbacbdf/cross-boundary_data_flow/index.html> (accessed 7 May 2025).

the group. Most countries recognise intra-group agreements as a type of contract-based transfer mechanism, but not all countries recognise BCRs. Intra-group agreements are also easier to adopt since they are regarded as contract, while *ex-ante* regulatory approval may be required for BCRs, such as in the European Union ("EU"). The Asian Business Law Institute ("ABLI") has developed a framework for intra-group transfers based on the ASEAN MCCs.

B. Certifications

21 Certification mechanisms provide a more systematic solution that may either complement contracts[27] or, in some jurisdictions,[28] be recognised as a separate transfer mechanism. Significant investment of resources is required by businesses that wish to be certified. However, certifications can be a differentiator for businesses that process voluminous personal data, *eg*, cloud services, call centres and business process outsourcing services. Buyers of services often look to certification marks as a proxy for not merely that data protection standards are observed but also for the assurance that these are validated through periodic independent audits. Each business will make its own cost-benefit analysis to determine if the benefits of certification warrant the costs and resources required to obtain and maintain certification.

22 Certifications are supported under the DEPA in a couple of ways. Some countries, like Singapore, have a national data protection trustmark. The *recognition* of national trustmarks or certification frameworks is identified in the DEPA as a transfer mechanism that can be developed to promote interoperability.[29] The DEPA exhorts parties to encourage adoption of trustmarks and to mutually exchange best practices.[30] This presents an

27 The maintenance of certification can be a condition of a contract for data processing services.

28 Japan and Singapore recognise the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) certifications as standalone transfer mechanisms.

29 Digital Economy Partnership Agreement (6 November 2020) (entered into force 28 December 2020) Arts 4.2.6(c) and 4.2.10.

30 Digital Economy Partnership Agreement (6 November 2020) (entered into force 28 December 2020) Arts 4.2.8 and 4.2.9.

opportunity for mutual recognition of national trustmarks or certifications under national certification frameworks to be recognised as a standalone transfer mechanism. This means that there will be no need for lengthy contractual clauses that spell out the minutiae of data protection obligations. All that may be required is a simple contractual clause that makes the maintenance of the trustmark or certification a condition of the contract for data processing services.

23 There are also international certification frameworks, such as the Asia-Pacific Economic Cooperation ("APEC") Cross Border Privacy Rules ("CBPR") and Privacy Recognition for Processors ("PRP"), and the expanded framework for Global CBPR and PRP. There is potential for these international certification frameworks to be recognised as standalone transfer mechanisms under the DEPA, which identifies the development of broader international frameworks as one of the avenues that signatories can pursue for the development of transfer mechanisms to promote interoperability.[31] These certifications do not exist in isolation but are embedded within a broader international framework. For example, the Global CBPR framework establishes a set of privacy principles upon which the certification system is established.[32] The framework is also supplemented by a network for privacy enforcement cooperation.[33] The enforcement network gives teeth to the privacy principles and provides the means for mutual assistance when national data protection authorities need help to enforce cross-border data breaches.

31 Digital Economy Partnership Agreement (6 November 2020) (entered into force 28 December 2020) Art 4.2.6(b).

32 Namely, (a) preventing harm; (b) notice; (c) collection limitation; (d) uses of personal information (*ie*, purpose limitation); (e) choice; (f) integrity of personal information; (g) security safeguards; (h) access and correction; and (i) accountability. These principles are largely consistent with the DEPA privacy principles.

33 Global Cooperation Arrangement for Privacy Enforcement (CAPE).

C. Mutual recognition of equivalence

24 Finally, the DEPA includes an exhortation for signatories to develop other avenues of transfer of personal information.[34] This opens the door for more innovative transfer mechanisms. It cannot be gainsaid that mutual recognition that national legal systems for data protection are equivalent is a powerful example of government-to-government collaboration that brings the broadest benefits to bilateral trade and reduces compliance burdens for the greatest number of businesses, especially small and medium-sized enterprises with limited means for legal compliance. Assessment of national legal systems is not new: it started with EU adequacy assessments for dependent territories and former colonies, but even for the EU, this has recently evolved into (a less patronising) mutual recognition with trading partners such as Japan and South Korea.[35]

25 There is room for innovation in transfer mechanisms to support multilateral trade under the DEPA. It is possible to establish a framework for mutual recognition of equivalent protection at both national and subnational levels. The ABLI has published a think-piece for the establishment Trusted Data Corridors ("TDC") to link Special Economic Zones. The basic features of a Trusted Data Corridor are: First, the alignment of data protection standards by referencing a mutually agreed independent standard. Such standards may be international principles such as the OECD Privacy Principles or they could be regional principles such as the APEC Information Privacy Principles and the ASEAN Principles of Personal Data

34 Digital Economy Partnership Agreement (6 November 2020) (entered into force 28 December 2020) Art 4.2.6(d).

35 Directorate-General for Justice and Consumers, "Joint Press Statement on the Conclusion of the First Review of the Japan-EU Mutual Adequacy Arrangement" (4 April 2023) <https://commission.europa.eu/news/joint-press-statement-conclusion-first-review-japan-eu-mutual-adequacy-arrangement-2023-04-04_en> (accessed 7 May 2025); Directorate-General for Justice and Consumers, "Joint Press Statement by Haksoo Ko, Chairperson of the Personal Information Protection Commission of the Republic of Korea, and Didier Reynders, Commissioner for Justice" (31 October 2024) <https://commission.europa.eu/news/joint-press-statement-haksoo-ko-chairperson-personal-information-protection-commission-republic-2024-10-31_en> (accessed 7 May 2025).

Protection. Each participating country of the TDC can conduct self-assessment of how its legal framework for personal data protection aligns with the independent standard. In this way, bilateral or even multilateral assessments of equivalence can be made against a common mapping standard which is then shared. This design makes it a lot easier to scale the TDC when there are multiple countries involved. This approach has its roots in Art 17 of the OECD Privacy Principles, which contemplates that the Principles function as an independent mapping standard for assessing equivalence of protections between the data protection laws of two or more countries.[36]

26 Once equivalence of standards is assessed to be satisfied, each participating country of the TDC will implement within its legal system the mechanism to mutually recognise equivalent protection of personal data and remove regulatory requirements for cross-border transfers: *ie*, national treatment. Implemented in the ideal scenario, no other transfer mechanism will be necessary for data transfers within the TDC: businesses will no longer need to rely on contracts or certifications. The scope of coverage of a TDC, and accordingly such national treatment, can be national or be initially limited to specific areas, such as a Special Economic Zone. Taking incremental steps helps to build confidence and trust, which may pave the way for eventual expansion of coverage.

27 The establishment of enforcement cooperation for handling complaints and investigations into data incidents is an important aspect of the TDC. This extends beyond mutual assistance in the investigations into data breaches. There is also the need for mutual agreement to adopt international or industry standards for access to exported data by law enforcement, regulatory or judicial authorities, *eg*, Trusted Cloud Principles (Trusted Cloud Initiative) and OECD Declaration on Government Access to Personal Data Held by Private Sector Entities.[37] This

36 Article 17 expressly states that adherents to the OECD Privacy Principles should refrain from restricting transborder flows of personal data with countries that substantially observe those self-same principles.

37 OECD, *Declaration on Government Access to Personal Data Held by Private Sector Entities* (OECD/LEGAL/0487).

provides clarity to businesses operating within the TDC about the practices and procedural safeguards whenever there is a lawful need from public authorities to access exported personal data. An important aspect of procedural clarity is how access notices are served: the TDC contemplates that access notices are served directly on customers (*ie*, controllers or owners of data) and clarifies that data processors may notify affected customers when handling access requests.

VI. Conclusion

28 As more businesses and end users participate in the digital economy, there is greater need to ensure that cross-border transfers of data are seamless. Commercial relationships will increasingly be comprised predominantly, if not entirely, of data flows. The DEPA principles establish global norms for free flow of data and minimisation of restrictions; any restriction must be necessary, proportionate, fair and non-discriminatory. Where there are restrictions, such as those on personal data, governments should provide a broad range of solutions to help businesses comply and minimise business costs. The DEPA data module sets the standard for promoting interoperability and supporting innovation in the development of new transfer mechanisms. Innovation in technology and business models has given rise to the digital economy, so too must innovation in trade policy provide new avenues for data transfers.