EUI GLOBAL GOVERNANCE PROGRAMME

ROBERT SCHUMAN CENTRE

POLICY BRIEF

Data governance models and geopolitics: Insights from the Indo-Pacific region

Introduction

Cyberspace is widely recognised as an "object of geopolitical competition" between countries advocating for an open internet space and countries that aim to use this space as a tool for control.[1] The Indo-Pacific region represents one of the most contested and strategically significant domains, principally because of the role of China, which hosts the world's largest cohort of internet users and also the most sophisticated internet censoring and monitoring regime.[2]

Regulation of the internet has moved from attempting to regulate the flow of information into countries to also including attempts to regulate the data flowing out of countries, efforts which in both cases appear to have economic and political rationales that are often hard to disentangle.[3] The flow of information into a country can be regulated with different policies, including censorship and filtering (which can happen in different layers of the internet infrastructure) and also with market access restrictions, which can take the form of strict licensing regulations, joint-venture requirements, maximum foreign equity shares and nationality requirements which can apply to certain sectors sensitive to the spread of information, e.g. online news, social media and blogs,

1 Deibert, R. (ed.) (2012), *Access contested: security, identity, and resistance in Asian cyberspace information revolution and global politics*, Cambridge, MA: MIT Press.

2 The term Indo-Pacific region is commonly used to refer to the region going from the Indian Ocean to the Pacific Ocean, although there are variations in definitions. In this policy brief, I focus on 15 economies in the region, namely Australia, China, Hong Kong, India, Indonesia, Japan, Korea, New Zealand, Pakistan, the Philippines, the Russian Federation, Singapore, Taiwan, Thailand and Vietnam.

3 Chander, A. and Lê, U. (2015) 'Data Nationalism,' Emory Law Journal, 64(3), p. 677.

Author

Martina Francesca Ferracane | European University Institute

Issue 2022/48
September 2022

among others. On the other hand, the flow of information out of a country can be restricted through regulation of the processing and transfer of data, which can consist in requiring certain data to be processed within the borders of the country or companies to meet certain conditions before data can be transferred abroad.

Regulation of cross-border data flows has become a major focus of geopolitical contestation, reflecting the importance of data as a strategic asset in the digital era and the symbolic importance data privacy and security have assumed in general discourse on democracy vs autocracy. This paper characterises the data policies that apply in 15 Indo-Pacific economies and the emerging pattern of bilateral and plurilateral cooperation on cross-border data flows. A premise of the analysis is that differences in data regulation and the patterns and types of international cooperation between states provide insights into the inclusive and exclusive geopolitical dynamics in the region.

Data policies in the Indo-Pacific region: an overview

This section provides an overview of the data governance models applied in 15 Indo-Pacific economies to different types of data. The analysis is based on policies listed in the upcoming Digital Trade Integration Database of the European University Institute.[4]

Australia

The My Health Records Act of 2012 is the only measure limiting the flow of data from Australia to the rest of the world. Section 77 of the Act requires information relating to health records to be stored and processed within Australia unless the records do not include "personal information in relation to a healthcare recipient or a participant in the My Health Record System" or "identifying information of an individual or entity." The country has had a data protection law in place since 1988 (Privacy Act 1988). In 2012, certain privacy principles were inserted into the Privacy Act. Privacy Principle 8 creates a regime that allows cross-border disclosure of personal information in six different scenarios, including situations in which there are data protection frameworks that are similar or equivalent to that in Australia, in which there is consent to the disclosure and in which the disclosure is required by law. Overall, these conditions are very wide and are not found to restrict the movement of data.

China

As China has been "unwilling to accept a cyberspace determined by others," it has worked towards "asserting a more ambitious foreign policy for cyberspace" (Deibert, 2012). The country has implemented an intricate web of restrictions on different types of data. These policies started to be implemented in the early 2000s and cover different sectors and types of data.

The "Notice to Urge Banking Financial Institutions to Protect Personal Financial Information" of 2011 states that the personal information collected by commercial banks must be stored, handled and analysed within the territory of China and such personal information is not allowed to be transferred overseas. In addition, the more recent Personal Financial Information Protection Technical Specification (PFI Specification) of 2020 regulates "any personal information collected, processed and stored by financial institutions during the provision of financial products and services," requiring that personal financial information (PFI) collected or generated in mainland China be stored, processed and analysed within the territory. Where there is a business need for cross-border transfer of PFI and the financial institution obtains explicit consent to the transfer from the personal financial information subjects (i.e. the persons under the PFI Specification providing the data), it must conduct a security assessment and then supervise the offshore recipient to ensure responsible processing, storage and deletion of PFI.

The Administrative Measures for Population Health Information (for Trial Implementation) of 2014 require that population health information be stored and processed within China. In addition, storage is not allowed overseas. Other restrictions apply to map services and the online taxi sector. The Map Management Regulations require that online map providers set up their server inside the country and must acquire an official certificate, while according to the Interim Measures for the Administration of Online Taxi Booking Business Operations and Services, online taxi companies must store and use personal information and business data in mainland China and cannot transfer the data outside China.

The Cybersecurity Law requires that the personal information of Chinese citizens and important data collected by critical information infrastructure operators (CIIOs) in mainland China be stored within mainland China. Where due to business requirements it is truly necessary to provide such informa-

4 https://globalgovernanceprogramme.eui.eu/digital-trade-integration/

tion outside China, CIIOs must employ measures jointly formulated by the state cybersecurity and informatisation departments and the relevant departments of the State Council to conduct a security assessment, and where laws and administrative regulations provide otherwise they must follow those provisions. As a result, it is reported that in February 2018 Apple began hosting Chinese users' iCloud accounts, along with their encryption keys, in a Chinese data centre to comply with these new measures.

Additionally, the Draft Measures for the Security Assessment of Outbound Transmission of Personal Information and Critical Data (Draft Measures) issued in April 2017 by the Cyberspace Administration of China would expand this restriction to all "network operators." This expands the scope of the measure to cover most, if not all, cloud service providers. The draft measures allow some smaller organisations (or smaller transfers) to be subject to a simple self-assessment regime as long as the data they seek to transfer are not deemed relevant to national security or social and public interest. However, larger organisations and larger transfers (e.g. over 500,000 records) must be assessed by the competent authority.

In lieu of the Draft Measures, the Cyberspace Administration of China (CAC) has opted to apply two separate sets of security assessment requirements for the outbound provision of personal information and important data. These are the 'Draft Administrative Measures on Data Security' and the 'Draft Measures for Security Assessment of Exports of Personal Information'.

Additionally, a Personal Information Security Specification which came into force in May 2018 further cements the need for security assessments when outsourcing data processing to a third party and mandates the need for audits and contractually obligated security measures. Furthermore, a 2020 Specification states that personal information controllers (any private or public organisation that has "the power to decide the purpose and method" of processing personal information) shall when entering into business arrangements with third parties which collect information on employees or consumers require that such third parties collect personal information by legal means with the necessary consent. The 2020 Specification advises personal information controllers to make technical tests of third parties' embedded automation tools, such as codes, scripts, interfaces, algorithm models and software development kits, and immediately disconnect them if the personal information collected by the third party exceeds the agreed scope.

Hong Kong

In 1995 Hong Kong was among the first Asian jurisdictions to enact comprehensive personal data privacy legislation and to establish an independent privacy regulator. Under Section 33 of the Personal Data (Privacy) Ordinance, there are prohibitions on the transfer of personal data to places outside Hong Kong except in specified circumstances. However, this section has not yet come into operation.

India

India started to restrict transfers of data across borders in 2012. The first measures implemented covered government activities. The National Data Sharing and Accessibility Policy of 2012 requires that "non-sensitive data available either in digital or analogue forms but generated using public funds" must be stored within the borders of India. The policy states that data belong to the "agency/department/ministry/entity which collected them and reside in their IT enabled facility." In 2015, India's Ministry of Electronics and Information Technology (MEITY) issued guidelines for a cloud computing empanelment process in which cloud computing service providers may be provisionally accredited as eligible for government procurements of cloud services. The guidelines require such providers to store all data in India to qualify for the accreditation.

In the years 2017 and 2018 two new regulations were implemented in the financial and insurance sectors. The Insurance Regulatory and Development Authority of India Regulations of 2017 provide that Indian insurers, even in cases where they outsource their services outside India, must retain all original policy-holder records in India. In April 2018, the Reserve Bank of India (RBI) issued a one-page directive stating that within six months all payment data held by payment companies should be held in local facilities. The directive notes that this would help the RBI gain "unfettered supervisory access" to transaction data, which it needs to ensure proper monitoring. Following a negative response from international payment companies such as MasterCard, Visa and American Express, the RBI proposed to ease this restriction so as to allow payment firms to store data offshore, as long as a copy is kept in India. With respect to the processing of domestic payment transactions taking place outside India, the RBI requires that the data must only be stored in India after processing and should be

deleted from systems abroad and brought back to India no later than 24 hours after processing.

Although there is no standalone and comprehensive privacy law in India, the Information Technology Act 2000 read together with the supplementary Information Technology Rules acts as the legal cornerstone to ensure the protection of personal information and imposes certain conditions for personal data transfers. The rules provide that cross-border data flows of sensitive personal data or information can be made to any other corporate entity or person in India or to any other country that ensures the same level of data protection as provided under the rules and provided that the transfer is necessary for the performance of a lawful contract between the corporate body (or any person acting on its behalf) and the provider of information, or provided that such transfer has been consented to by the provider of the information. Sensitive personal information includes passwords, financial information such as bank account or credit/debit card details, sexual orientation, physical and mental health conditions and biometric information, among other things.

A Personal Data Protection Bill (PDPB 19) introduced in Parliament in December 2019 is currently under consideration. Under the proposal data transfers abroad may take place in a tiered system whereby personal data can be transferred, while "sensitive data" for processing may be transferred with prior authorisation by a Data Protection Authority (DPA) and with a mirror copy located in the country.[5] "Critical personal data" bearing on India's security interests (to be defined by the central government) must be stored and processed locally. The prospect of a Personal Data Protection Bill has been much debated in India.

Indonesia

Indonesia imposes restrictions on transfers of health and financial data and also on electronic system operators in public service. Government Regulation No. 46/2020 mandates that health data should be stored in Indonesia, while Financial Services Authority (OJK) Regulation No.38/POJK.03/2016 requires foreign banks and payment networks to locate their data centres and process electronic transactions in Indonesia.

In addition, Government Regulation No. 71/2019 states that electronic system operators for public scope should store electronic transaction data in Indonesia. The Regulation defines public electronic system operators as (a) public bodies (such as central and regional executive, legislative and judicative bodies and any other bodies established pursuant to a statutory mandate); and (b) entities appointed by public bodies to operate electronic systems on their behalf. Previously, Government Regulation 82 (Article 17) required "electronic system operators for public service" to connect their data to a data centre and a disaster recovery centre established in Indonesian territory for law enforcement and data protection. Although 'public service' was not defined in GR 82, in practice the term was broadly interpreted by the Ministry of Communication and Informatics (MOCI). Therefore, the local storage obligation was widely understood to cover all services offered to the public via the internet, effectively affecting many private sector companies.[6]

While Government Regulation No. 71/2019 abolished the local processing requirement for electronic system operators for private scope, it is subject to certain conditions: that the location of the electronic system and electronic data outside Indonesia does not diminish the effectiveness of supervision by relevant state ministries, institutions and law enforcement agencies; and that access to the electronic system and electronic data must be provided for the purpose of supervision and law enforcement in accordance with the law.

Two regulations apply to the processing of personal data at the horizontal level. MOCI Regulation No. 20 of 2016 stipulates that consent from the data subject is necessary for the transfer of data. This consent must be in Bahasa Indonesia (or in bilingual format) and collected online or on paper hardcopy. The Regulation also mandates that personal data that is electronically stored should be encrypted. Under Government Regulation No. 71/2019, consent must be obtained from data subjects for cross-border transfers of personal data. This consent must be "lawful consent," i.e. consent that is delivered explicitly, cannot be concealed and is not based on error, negligence or coercion.

Sectoral regulation on personal data includes Government Regulation No. 80/2019, which states that personal data held on e-commerce platforms can-

5 https://www3.weforum.org/docs/WEF_Data_Flow_Governance_2021.pdf

6 https://sites-herbertsmithfreehills.vuturevx.com/208/26111/compose-email/cross-border-data-transfers--an-indonesian-law-update.asp

not be sent overseas unless the relevant ministry confirms that the foreign country has the same level of personal data protection as Indonesia, and Circular Letter No.14/SEOJK.07/2014 from the Financial Service Authority (OJK), which stipulates that financial service institutions should not disclose their customers' data to third parties without consent from the data owner. The consent should be expressed in writing.

Japan

Japan does not impose any restrictions on transfers of data across borders, except for conditions applied to transfers of personal data since 2017. The Act on the Protection of Personal Information (Act No. 57 of 2003) (APPI) did not originally restrict transfers of personal information to foreign countries, but amendments enacted in 2015 which took effect in May 2017 added conditions on cross-border flows of personal data which resemble the conditions in the EU General Data Protection Regulation (GDPR).

Republic of Korea

Despite provisions in its FTAs with the EU and the US allowing financial data to be sent across borders, for several years Korea prohibited outsourcing of data-processing activities to third parties in the financial services industry and certain restrictions still apply. Banks could therefore only process financial information related to Korean customers in-house, either in Korea or abroad, and offshore outsourcing was restricted to a financial firm's head office, branches and affiliates. In June 2015, the Financial Services Commission (FSC) revised its regulations to: eliminate the approval process for the outsourcing of IT facilities; lift restrictions on third-party outsourcing or re-outsourcing; establish a broader application of *ex post facto* reporting requirements to process consumer and corporate transaction data; and abolish the Financial Supervisory Service security review in the application process.

The Credit Information Use and Protection Act permits transfers of financial information for the purpose of outsourcing ("entrusting") but some limitations remain in relation to processing credit information and unique identification information (e.g. resident registration numbers, driving licence numbers, passport numbers and alien registration numbers).

Certain restrictions also apply to location data, mainly in connection with political tension with North Korea. Article 16 of the Act on the Establishment, Management etc. of Spatial Data provides that geographical data related to maps or photos produced for the purpose of a survey cannot be transferred abroad except with permission from the Minister of Land, Infrastructure and Transport. This provision has been in place since 2014. In addition, under Article 5 of the Act on the Protection, Use etc. of Location Information, any person who intends to engage in the location information business must obtain permission from the Korea Communications Commission. Even if they are permitted to do such business, Article 18 provides that location information providers and location-based service providers cannot collect individuals' location information without the individuals' consent. These restrictions have been in place since 2005. It has been reported that, although a supplier may export location information once it has acquired a permit, Korea has never approved a permit despite numerous applications by foreign suppliers in the last decade.[7]

The Personal Information Protection Act (PIPA), which was enacted in 2011 and recently amended in December 2020, creates a conditional flow regime in which a data controller is only required to obtain the consent of data subjects if they transfer data not "within a scope reasonably related to the original purpose of collection" (Article 26). "A scope reasonably related to the original purpose of collection" includes outsourcing personal information. The PIPA allows information and communication (IT) service providers to make cross-border transfers of personal information to jurisdictions with a comparable policy on cross-border transfers of personal information (Articles 39-13).

New Zealand

New Zealand applies limited restrictions on storing in the country a copy of certain tax records, accounting data and internal company records. These requirements can be found in Section 22(2) of the Tax Administration Act 1994, Sections 215 and 216 of the Financial Markets Conduct Act 2013, Section 189 of the Companies Act 1993, Section 75 of the Goods and Services Tax Act 1985 and the 2010 Revenue Alert 10/02 by the Commissioner of the Inland Revenue.

The new Privacy Act 2020, which entered into force in December 2020, creates a conditional flow regime for personal data. Information privacy princi-

7 https://ustr.gov/sites/default/files/2020_National_Trade_Estimate_Report.pdf

ple 12 in Section 22 of the Act governs cross-border data transfers. A business or organisation may only disclose personal information to another organisation outside New Zealand if the receiving organisation: is subject to the Privacy Act because it does business in New Zealand; is subject to privacy laws that provide safeguards comparable to the Privacy Act or it agrees to protect the information in a similar way (e.g. by using model contract clauses); is covered by a binding scheme; or is subject to the privacy laws of a country prescribed by the New Zealand Government.

Pakistan

Pakistan does not impose any restrictions on cross-border transfers of data except that it prohibits data transfers to countries that it does not recognise, including Israel, Taiwan, Somaliland, Nagorno, Karabakh, Transnistria, Abkhazia, Northern Cyprus, the Sahrawi Arab Democratic Republic, South Ossetia and Armenia. In addition, data transfers to India must be justified by the transferor.[8]

The country does not have a data protection law in place but it has implemented certain sectoral data protection laws. It is reported that data collected by banks, insurance firms, hospitals, defence establishments and other 'sensitive' institutions may not be transferred to any individual or body without authorisation from the relevant regulator on a confidential basis.[9]

The Philippines

The Philippines have virtually no restriction on cross-border transfers of data, as the country follows the principle of accountability (Chapter IV of the Republic Act 10173 – Data Privacy Act of 2012).

The Russian Federation

Together with China, the Russian Federation is one of the countries with the highest level of controls on cross-border data transfers. The restrictions cover different sectors and types of data. In July 2006 Federal Law No. 152-FZ implemented comprehensive regulation of personal data. In July 2014, the law was amended by Federal Law No. 242-FZ to include a strict requirement that data should be processed locally. Article 18.5 requires data operators to ensure that the recording, systematisation, accumulation, storage, update/amendment and retrieval of personal data of citizens of the Russian Federation is made using databases located in the Russian Federation. This amendment entered into force on 1 September 2015. Online websites that violate this prohibition can be placed on the Roscomnadzor's blacklist of websites. Once personal data are collected, they are to be put in a database located in Russia (i.e. the primary database) so that all operations on the data are carried out locally. Afterwards, the data can be transferred abroad for further processing (i.e. to a secondary database). Since December 2019, the administrative penalty for a data operator not complying with the local processing requirement has amounted to from 1 million to 6 million Russian roubles for an initial violation and the fine can be from 6 million to 18 million Russian roubles for repeated violations. The fine for managers responsible for violations varies between 100,000 and 200,000 Russian roubles for initial violations and between 500,000 and 800,000 roubles for repeated violations.

Certain restrictions also apply to data on international payments. Federal Law No. 161-FZ 'On the National Payment System' as amended in October 2014 by Federal Law No. 319-FZ required international payment systems to transfer their capabilities to process Russian domestic operations to the local state-owned operator (National Payment Card System) by 31 March 2015.

Other restrictions include local storage for a period of at least six months of certain user data processed by internet service providers (ISPs) in relation to public Wi-Fi user identification in public places including parks, hotels, cafes, restaurants, clubs, cinemas and shopping centres. Law No. 97-FZ and relevant Government decrees require that ISPs should identify internet users by means of identity documents (such as passports) and identify terminal equipment by determining the unique hardware identifier of the data network.

In addition, Federal Law No 374-FZ requires telecom operators and ISPs to store locally information confirming the receipt, transmission, delivery and/or processing of voice data, text messages, pictures, sounds, video and other communications (i.e. metadata reflecting these communications).

Finally, Federal Law No. 152-FZ implements a conditional regime for transfers of personal data outside Russia. Transfers of personal data outside Russia

8 No legislative text has been found regarding this measure. However, this situation has been reported by the law firm DLA Piper. See DLA Piper (2021).

9 *Ibid.*

only do not require additional consent from the data subject if the jurisdiction that the personal data are transferred to ensures adequate protection of such data. These jurisdictions are the countries that are parties to the Council of Europe's Convention for the Protection of Individuals regarding Automatic Processing of Personal Data and other countries approved by the Russian Federal Service for Supervision of Communications, Information Technologies and Mass Media (Roskomnadzor). Roskomnadzor's official list of such countries is: Australia, Bangladesh, Belarus, Benin, Canada, Costa Rica, Gabon, Israel, Japan, Kazakhstan, Malaysia, Mali, Mongolia, New Zealand, Niger, Nigeria, Peru, Qatar, Singapore, South Africa, South Korea, Tajikistan, the Togolese Republic, Uzbekistan, Vietnam and Zambia.

Singapore

When it comes to data protection Singapore employs a model similar to the European Union's GDPR. The Personal Data Protection Act 2012 contains restrictions on offshore transfers which require organisations to ensure that the receiving organisation has in place "comparable protection" to the standards set out in the Act when transferring personal data outside Singapore. The mechanisms to achieve this include data transfer agreements, individual consent and justification of the transfer in certain prescribed circumstances, including in connection with the performance of contracts between the transferring organisation and an individual, subject to certain conditions being met.

Taiwan

Taiwan imposes restrictions on transfers of data to mainland China. In September 2012, the National Communications Commission issued an order prohibiting communication business operators from transferring personal data of other users to the mainland. The blanket order prohibits communication enterprises (i.e. telecom carriers and broadcasting operators) from transferring subscribers' personal data to mainland China on the ground that the personal data protection laws in mainland China are still inadequate.

When it comes to personal data, the Personal Data Protection Act of 1995 imposes a conditional regime. Under Article 21 of the Act, the government may impose restrictions on a cross-border transfer of personal data by a non-government agency if: major national interests are involved; an international treaty or agreement so stipulates; the country receiving the data lacks proper regulations on the protection of personal data and the data subject's rights and interests may be consequently harmed; the transfer to a third country is carried out to circumvent the Act.

A conditional regime also applies to financial data. Article 18 of the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation (promulgated in 2006) deals with the conditions under which a financial institution may outsource its operations to an overseas service provider. The financial institution must obtain a confirmation letter from the financial authority of the country where the outsourced services are conducted agreeing to the outsourcing operation. In addition to the confirmation letter, a foreign bank branch in Taiwan must obtain a letter authorised by its head office or regional head office consenting to it obtaining and using the data, and to security control and cooperation with the supervisory requirements in Taiwan.

Thailand

Thailand imposes local processing restrictions on credit information under the Credit Information Business Act of 2002. Chapter 2 of the Act states that only a credit information company has the right to operate a credit information business (Section 9) and that "No credit information company or information controller or information processor carrying on or operating the business in the Kingdom shall operate, control or process information outside the Kingdom" (Section 12).

In addition, Thailand imposes a conditional regime similar to the EU GDPR. According to Part 3 of the Personal Data Protection Act 2019 (PDPA), transfers of data outside Thailand are only allowed if the destination country has adequate data protection standards or approaches. There are four exceptions to the adequacy requirement in the law: the data subject's consent to the transfer has been obtained; specific statutory exemptions apply; the receiving organisation provides suitable protection measures that enable enforcement of the data subject's rights; and the receiving organisation has put in place a "personal data protection policy" applicable to overseas data transfers.

Vietnam

Vietnam imposes restrictions on a wide range of data. Decree No. 72 on the management of internet services and online networks requires providers of websites, social networks, information on mobile networks and online games to have at least one

server inside the country "serving the inspection, storage, and provision of information at the request of competent state management agencies" (Articles 22, 25, 28 and 34). In March 2018, the Vietnamese government issued Decree No.27/2018/ND-CP to partially amend and enhance Decree 72, but the local server requirement remains.

In February 2020, the Vietnamese government issued Decree No.15/2020/ND-CP to regulate administrative violations in post-telecommunications, radio frequency, IT and electronic transactions. Article 44.1.(d) of the Decree regulates penalties for electronic newspapers, general websites, web portals and social networks subject to a licence for not storing information in a server system with a Vietnamese IP address. Article 95.3 regulates penalties for advertising email and internet message services using servers not located in Vietnam.

On 12 June 2018, the Vietnamese government issued Law No. 24/2018/QH14 on Cybersecurity (Law No. 24/2018/QH14). Article 26 of the law requires foreign providers of internet services, telecom services and value-added services to open representative offices or branches in Vietnam and to domestically store the personal information of Vietnamese users and users within Vietnam.

The country does not have a comprehensive regulation on the protection of personal data, but there are a set of fragmented sectoral regulations, including the Law on Network Information Security (Law No. 86/2015/QH13), Law No. 24/2018/QH14 on Cybersecurity and the Law on Information Technology.

Data policies as a geopolitical arena

The above analysis of data policies in the Indo-Pacific region shows that national data governance models diverge widely. Ferracane and van der Marel (2021) identify three main models of data governance: an open model with unrestricted transfers of data; a conditional model in which data can only flow freely if certain requirements are met; and a control model in which significant restrictions are imposed on data transfers.[10] While the models were developed in relation to personal data, they can be extended to all types of data. In fact, countries may apply different governance models to different types of data. Table 1 summarises the data models applied by the 15 Indo-Pacific economies analysed in the previous section.

10 Ferracane, M.F. and van der Marel, E. (2021), *Regulating Personal Data: Data Models and Digital Services Trade*, Working Paper. Washington, DC: World Bank. doi:10.1596/1813-9450-9596.

Table 1: Summary of data models applied in the 15 Indo-Pacific countries

	Open model	Conditional model	Control model
Hong Kong	All data		
Philippines	All data		
Pakistan	All data except to selected countries		Transfers to countries not recognised (Israel, Taiwan, Armenia and others)
Australia	All data except health data and personal data	Light conditions on personal data	Health data
Japan	All data except personal data	Personal data	
Singapore	All data except personal data	Personal data	
New Zealand	All data except personal data and certain tax data	Personal data, tax data	
Thailand	All data except personal data and credit information	Personal data	Credit information
Korea	Other data	Personal data	Location-based services, credit information
Taiwan	Other data	Personal data, financial data	Transfers to mainland China of user data by communication companies
India	Other data	Personal data	Data generated using public funds, cloud public procurement services, payment data
Indonesia	Other data	Electronic systems operators, e-commerce	"Electronic systems operators for public service," health data, financial sector data
Russian Federation	Other data		Personal data, financial sector data, user data saved by ISPs providing public Wi-Fi, user data saved by telecommunication operators, ISPs and message exchange services
Vietnam	Other data		Providers of websites, social networks, information on mobile networks and online games, post-telecommunications, radio frequency, IT and electronic transactions, personal information of users of internet services, telecom services and value-added services
China	Other data	Personal data	Financial data, personal data, data collected by "critical information infrastructure operators," health data, critical data, online taxi sector data, map services

Source: EUI Digital Trade Integration database (forthcoming).

The summary table suggests that three groups of countries can be associated with each data governance model, although the borders between the groupings are fuzzy given that policies vary across types of data and sectors. In four countries – Australia, Hong Kong, Pakistan and the Philippines – the open data governance model is prevalent. Seven economies – India, Japan, Korea, New Zealand, Singapore, Taiwan and Thailand – mostly have a conditional model, but with some exceptions for sensitive data. In China, Indonesia, the Russian Federation and Vietnam transfers of most types of data are heavily regulated and controlled. In the sample, Indonesia and Korea are the only countries that have liberalised their data regimes by lifting specific restrictions on cross-border data transfers, although certain limitations still apply. In both cases, the change of policy was related to commitments made in free trade agreements (FTAs).[11]

As Ferracane and van der Marel (2021) show, each data model is centred around a large economic market. Trade among countries sharing the open model takes place mainly with the United States, trade among countries sharing the conditional model is in great part driven by the European Union, and trade among countries sharing the control model is guided by China.

While the choice to apply a certain data governance model will be driven by both economic and political factors, analysis of the data governance models in the region suggests there are geopolitical forces at play.

Commitments made by Indo-Pacific countries in bilateral and regional free trade agreements or data-specific cooperation initiatives provide additional insights into the role of geopolitics. Table 2 summarises commitments on data flows made in international agreements by the 15 economies analysed with respect to data flows. The first three columns show commitments made in agreements by countries that apply the open data model, which is strongly advocated by the United States. The fourth column shows which countries have obtained a so-called data adequacy decision from the European Union, which is the driver of the 'conditional model' and is active in exporting this model to the rest of the world.[12] Data adequacy decisions are premised on a determination by the European Commission that a partner country's data protection regime is equivalent to that of the EU. The last two columns show whether the countries participate in lighter non-binding commitments on data flows, an approach advocated by China.

11 Korea removed restrictions on financial data following commitments made in the FTA with the United States, which entered into force in March 2012, and the FTA with the European Union, which entered into force in July 2011. Indonesia removed some of its restrictions after the entry into force of the 2019 Indonesia-Australia Comprehensive Partnership Agreement.

12 This is an example of what has been called the 'Brussels effect.' See Bradford, A. (2020), "The Brussels Effect: How the European Union Rules the World," Oxford University Press, New York, NY.

Table 2: Commitments on data flows by Indo-Pacific countries

	APEC CBPRs	CPTPP	Other binding commitments on data flows	EU adequacy	RCEP	Other non-binding commitments on data flows
Hong Kong			✓			✓
The Philippines	✓				✓	✓
Pakistan						
Australia	✓	✓	✓		✓	✓
Japan	✓	✓	✓	✓	✓	✓
Singapore	✓	✓	✓		✓	✓
New Zealand		✓	✓	✓	✓	✓
Thailand					✓	✓
Korea	✓			✓	✓	✓
Taiwan	✓					✓
India						✓
Indonesia			✓		✓	✓
China					✓	
Russian Federation						
Viet Nam		✓			✓	✓

Source: Author compilation based on data from the TAPED database.[13]

The APEC Cross-Border Privacy Rules (CBPRs) in the first column of the table are a government-backed data privacy certification framework that companies can join to demonstrate compliance with agreed privacy protection principles and enforcement mechanisms, allowing them to transfer data between CBPR-participating economies with greater trust. They reflect the open data model advocated by the United States as there are no restrictions applied to transfers of data across borders following a self-assessment of data policies by the company. Australia and Taiwan are the latest economies to participate, joining Canada, Japan, the Republic of Korea, Mexico, Singapore and the United States.

The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) includes substantive rules on cross-border data transfers stipulating that cross-border data transfers will not be restricted while allowing the parties to maintain measures that achieve legitimate public policy objectives provided the measures are non-discriminatory and not unnecessarily trade-restrictive. The CPTPP is the first agreement in which binding language on data flows was agreed and some Asian economies were its main advocates after the US pulled out from it during the Trump administration.[13] The agreement entered into force in 2018 and it covers Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam.

The third column indicates which countries have made horizontal binding commitments on free transfers of data following the model of the CPTPP. Among the agreements there is the Digital Economic Partnership Agreement (DEPA) signed in June 2020, which is the first digital-only deal. The DEPA members – Chile, New Zealand and Singapore – upheld their existing CPTPP commitments to allow data to flow freely across their borders (4.3)

13 The CPTPP is identical to the TPP text with only minor changes. It was agreed in 2015. When Trump withdrew the United States from participation in it in January 2017, Japan and New Zealand took the leadership role in the negotiations among the remaining participants.

and to prohibit data rules requiring local hosting of data (4.4) with improved clarity on the exceptions to both. It is a non-binding undertaking to deepen cooperation in the digital economy and represents a flexible scalable platform to build digital principles and standards to promote trust, efficiency and interoperability.[14] In October 2021, Korea formally requested to join the DEPA. Other agreements with binding commitments on data flows that include one or more of the 15 Indo-Pacific economies are: the updated Singapore-Australia FTA, which entered into force in December 2017; the Sri Lanka-Singapore FTA, which entered into force in May 2018; the Australia-Hong Kong FTA, which entered into force in January 2020; the Agreement between the United States of America and Japan concerning Digital Trade, which entered into force in January 2020; the Australia-Peru FTA, which entered into force in February 2020; the Indonesia-Australia Comprehensive Economic Partnership Agreement (CEPA), which entered into force in May 2020; the UK-Japan Comprehensive Economic Partnership Agreement, which entered into force in January 2021; and the Digital Economy Agreement (DEA) between the United Kingdom and the Republic of Singapore, which entered into force in June 2022 and updated the FTA between the two countries.[15]

With the exception of Vietnam, which joined the CPTPP but has a grace period of five years to comply with the provisions on data transfers, and Indonesia, which recently signed the Indonesia-Australia CEPA, the agreements associated with the open data governance model encompass countries with either an open data governance model or a conditional data model. These agreements tend to be more common among countries with a conditional data governance model than those with an open data model.

The fourth column lists countries that have received an adequacy decision from the European Commission. While New Zealand obtained an adequacy decision in 2012,[16] the other two decisions are more recent and show a renewed EU interest in strengthening relations with like-minded economies in the Indo-Pacific region. Adequacy status was granted to Japan in 2019 in a mutual recognition of adequacy status as Japan also recognised the EU as adequate on the same day. Japan adopted a conditional regime in 2015 with an amendment to the Personal Information Protection Act that became effective in May 2017. The third country in the region that has received adequacy is Korea, which was granted it in December 2021, although Korea had already adopted a conditional regime in 2011 with its Personal Information Protection Act. In all three cases, adequacy was granted to countries that already had FTAs with the EU although commitments on data flows were not part of these FTAs.[17]

The fifth and sixth columns in the table indicate non-binding commitments made by the 15 countries analysed. Column 5 refers to the Regional Comprehensive Economic Partnership (RCEP), which includes the first commitment by China to rules on data flows. The commitment is non-binding because there are significant exceptions in the agreement that allow the signatories to impose regulatory restrictions when they deem this necessary. Moreover, the agreement excludes the possibility of invoking dispute-settlement proceedings.[18] Nevertheless, the agreement is ground-breaking in its scope with the signatories representing 30 percent of global GDP.[19]

The last column covers other agreements with non-binding language on data flows that have been signed by at least one of the 15 countries analysed. These are: the FTA between the Republic of China (Taiwan) and the Republic of Nicaragua, which

14 Goodman, M.P. and Risberg, P. (2021), 'Governing Data in the Asia-Pacific.' Centre for Strategic and International Studies (CSIS).

15 The New Zealand-UK FTA has been signed but has not yet entered into force, while the Korea-Singapore Digital Partnership Agreement was agreed in December 2021 but has not yet been officially signed.

16 New Zealand amended its data protection law in 2020 to implement a conditional regime. Previously the country had an open regime with limited safeguards.

17 The Agreement between the European Union and Japan for an Economic Partnership allows the parties to reassess the need for the inclusion of provisions on the free flow of data in the Agreement. In July 2022, the European Commission requested the Council of the EU to authorise opening negotiations on the inclusion of provisions on cross-border data flows in the Agreement. See https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=COM:2022:336:FIN

18 Ferracane, M.F. and Li, M. (2021) 'What kinds of rules are needed to support digital trade?' in Rebooting multilateral trade cooperation: perspectives from China and Europe. London, UK: CEPR Press, pp. 153-175.

19 Australia, Brunei, Cambodia, China, Indonesia, Japan, Korea, Laos, Malaysia, Myanmar, New Zealand, the Philippines, Singapore, Thailand and Vietnam.

entered into force in January 2008; the New Zealand-Hong Kong China Closer Economic Partnership Agreement, which entered into force in January 2011; the FTA between the Republic of Korea and Peru, which entered into force in August 2011; the FTA between the United States of America and the Republic of Korea, which entered into force in March 2012; the FTA between Canada and the Republic of Korea, which entered into force in January 2015; the Agreement between Japan and Mongolia for an Economic Partnership, which entered into force in June 2016; the Agreement between the European Union and Japan for an Economic Partnership, which entered into force in February 2019; the ASEAN Agreement on Electronic Commerce, which entered into force in December 2021; the Protocol to Upgrade the FTA between the Government of the People's Republic of China and the Government of New Zealand, which entered into force in April 2022; and the CEPA between the Government of the Republic of India and the Government of the United Arab Emirates (UAE), which entered into force in May 2022.

Other important initiatives that are under discussion and are worth mentioning are the Cross-Border Data Transfer Mechanism proposed by ASEAN in early 2021 using model contractual clauses to legally transfer data outside ASEAN countries (Brunei, Myanmar, Cambodia, Timor-Leste, Indonesia, Laos, Malaysia, the Philippines, Singapore, Thailand and Vietnam) and the recently launched Indo-Pacific Economic Framework for Prosperity, which is intended to counter China's growing influence in the region and includes Australia, Brunei, India, Indonesia, Japan, Republic of Korea, Malaysia, New Zealand, the Philippines, Singapore, Thailand and Vietnam.

What next?

Over the past decade, three data governance models have emerged, all of which have gained traction in the Indo-Pacific region. While the 15 countries analysed apply different data governance models for different types of data and sectors, it is nevertheless possible to identify the main model each applies.

The open model, traditionally advocated by the United States, appears to be the main model of reference for Australia, Hong Kong, the Philippines and Pakistan. Most of the countries in the sample follow a conditional model, which resembles the EU approach to personal data regulation. These countries are: Japan, Korea, New Zealand, Singapore, Thailand, Taiwan and India. The 'control' model, of which China and the Russian Federation are the main advocates, appears to be a reference for Indonesia and Vietnam.

Analysis of commitments on data flows in the Indo-Pacific region shows that binding commitments are mostly made by countries with either the open or the conditional data transfer model. Although the European Union has never committed to a free flow of data in its free trade agreements (with the recent exception of the UK and perhaps also of Japan in the near future), countries that have adopted the conditional model have been the most active in undertaking these commitments. The three countries that have been granted adequacy by the European Commission have also signed agreements using US-inspired language on data flows, suggesting that countries do not need to choose between these two models. This is probably because the conditional approach to personal data has become common practice all over the world, and therefore policies à la GDPR are widely considered to constitute exceptions with a necessity to achieve a 'legitimate' policy objective.

Adoption of the control model is also not preventing countries from joining initiatives with binding commitments on data flows. In fact, Vietnam has joined the CPTPP, although it has a grace period of five years to comply with the provisions on data transfers, and Indonesia has recently signed the Indonesia-Australia CEPA, making binding commitments on data flows. This suggests that adopting different data models does not preclude cooperation and binding agreements on data flows. This is also illustrated by China's application to join the CPTPP, which represents an important opportunity to boost dialogue on data flows across geopolitical blocs.

The analysis also shows that non-binding international commitments are common among countries adopting any of the three data models. Of the 15 economies analysed, only two countries have not made any commitment on data flows, namely Pakistan and the Russian Federation, which respectively employ the open and the control data governance models. This suggests that common language on data flows at the regional level is within reach, representing an important step to consolidate the commitments undertaken in the RCEP and extend them to other countries in the region.

While the commitments on data flows are mostly embedded in trade agreements, more recently most of the progress has been taking place in 'digital trade agreements' like the DEPA and the US-Japan DTA, and in 'digital economy agreements,' which are politically binding but not legally binding. These more flexible mechanisms are designed to facilitate collaboration and prepare the ground for binding legal

commitments in future FTAs. The Joint Statement Initiative on E-commerce at the WTO (JSI) might be inspired by these novel approaches to overcoming geopolitical tensions on this contentious issue. The fact that India, a fierce opponent of the JSI, for the first time made a hortatory commitment on data flows in May 2022 allows hope for a potential inclusive discussion on cross-border data flows at the WTO.

The Global Governance Programme

The Global Governance Programme (GGP) is research turned into action. It provides a European setting to conduct research at the highest level and promote synergies between the worlds of research and policy-making, to generate ideas and identify creative an innovative solutions to global challenges. The Programme is part of the Robert Schuman Centre for Advanced Studies of the European University Institute, a world-reknowned academic institution. It receives financial support from the European Commission through the European Union budget. Complete information on our activities can be found online at: globalgovernanceprogramme.eui.eu

Robert Schuman Centre for Advanced Studies

The Robert Schuman Centre for Advanced Studies (RSCAS), created in 1992 and directed by Professor Erik Jones, aims to develop inter-disciplinary and comparative research on the major issues facing the process of European integration, European societies and Europe's place in 21st century global politics. The Centre is home to a large post-doctoral programme and hosts major research programmes, projects and data sets, in addition to a range of working groups and ad hoc initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration, the expanding membership of the European Union, developments in Europe's neighbourhood and the wider world.

www.eui/rsc

Co-funded by the
Erasmus+ Programme
of the European Union

© European University Institute, 2022
Editorial matter and selection © Martina Francesca Ferracane, 2022

This work is licensed under the Creative Commons Attribution 4.0 (CC-BY 4.0) International license which governs the terms of access and reuse for this work. If cited or quoted, reference should be made to the full name of the author(s), editor(s), the title, the series and number, the year and the publisher.

Views expressed in this publication reflect the opinion of individual authors and not those of the European University Institute.

Published by
European University Institute (EUI)
Via dei Roccettini 9, I-50014
San Domenico di Fiesole (FI)
Italy

doi:10.2870/487942
ISBN:978-92-9466-246-0
ISSN:2467-4540
QM-AX-22-048-EN-N