ECONSTOR
Make Your Publications Visible.

A Service of

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Khumon, Prapanpong

Conference Paper

Regulation for Cross-Border Privacy in Southeast Asia: An Institutional Perspective

29th European Regional Conference of the International Telecommunications Society (ITS): "Towards a Digital Future: Turning Technology into Markets?", Trento, Italy, 1st - 4th August, 2018

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Khumon, Prapanpong (2018) : Regulation for Cross-Border Privacy in Southeast Asia: An Institutional Perspective, 29th European Regional Conference of the International Telecommunications Society (ITS): "Towards a Digital Future: Turning Technology into Markets?", Trento, Italy, 1st - 4th August, 2018, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/184950

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

Regulation for Cross-Border Privacy in Southeast Asia: An Institutional Perspective

Prapanpong Khumon
Assistant Professor at the University of the Thai Chamber of Commerce
School of Law, 126/1 Vibhavadee Rangsit Road, Bangkok, Thailand, 10400
prapanpong_khu@utcc.ac.th

ABSTRACT

Free flow of cross-border data is important for a creation of a data-driven innovation. There is a global challenge on balancing business gains from unrestricted cross-border data flows with protection of personal data. While cross-border privacy is a global subject of regulation, only few countries in Southeast Asia have implemented data privacy laws. There have been initiatives in the region to harmonize rules on cross-border data transfers such as the APEC, the RCEP, and a newly proposed ASEAN e-commerce Agreement but they have not been concrete enough to offer a harmonization. The main challenge in the region is fragmentation since countries in the region accede to different instruments that have different principles on cross-border data privacy. Each jurisdiction still employs different standards on privacy protections. The lack of harmonized practices creates hurdles for intra-regional data transfers and protection of data privacy. The paper proposes a unifying approach for the region to avoid duplication with existing mechanisms. Rather than creating a new mechanism, the new approach will need to recognize and supplement compatibility with different frameworks. The proposed ASEAN Agreement on E-Commerce, expected to be finalized by the end of 2018, should carry out this unifying function to promote interoperability. In principles, it needs to be aligned with APEC's Cross Border Privacy Rules. A regional recognition scheme should be established to verify that a given country meets a sufficient level of personal data protection. There needs to be a technical assistance to developing countries that have limited resources in enacting and implementing data protection regulation.

KEYWORDS

Data privacy regulation, cross-border data transfers, Southeast Asia

1. INTRODUCTION

As global connectivity rises at an unprecedented level, cross-border data transfers and information sharing can facilitate economic activities of countries around the world. Global businesses now rely on data to be transferred freely to provide digital products and services across borders. Nevertheless, free flow of cross-border data increases risks of privacy infringement and cybersecurity threats. Certain governments also restrict free flow of cross-border data for legitimate reasons such as maintaining national security and prevention of immoral contents. Cross-border privacy has gained public attention following an annulment of safe harbor decisions by European Court of Justice in Maximillian Schrems v Data Protection Commissioner (2015)[1]

[1] Case C-362/14. Maximillian Schrems v Data Protection Commissioner [2015] ECLI: EU: C: 2015:650.

which declared that the US measures failed to provide adequate privacy protection of EU citizen's data being processed in the US. This decision leads to a renewed data privacy agreement between the EU and the US called the EU-US Privacy Shield, which strengthens levels of cross-border privacy protection between the two parties.

There is currently no global single agreement on data protection. While cross-border privacy is a global subject of regulation, only few countries in Southeast Asia have implemented data privacy laws[2], with the rest either having no regulation or in the process of developing one. Existing regulations on data privacy in certain Southeast Asian countries have similar principles with those of EU's General Data Protection Regulation (GDPR) in ensuring transparency and the right of data owners to access their data and to correct it. In terms of cross-border data transfers, countries such as Malaysia and Singapore may allow transfer of data to an organization outside their jurisdictions only when destination countries have adequate privacy protections comparable to protections granted under their own jurisdictions.[3] This is similar to the EU approach. However, while the EU has one single institution to adopt guidelines on adequate privacy protections (the European Commission), countries in Southeast Asia have different institutions and varying guidelines to carry out such purpose. For examples, Malaysia nominates Minister of Information, Culture and Communications to develop guidelines on adequate privacy protections[4] while Singapore's Personal Data Protection Commission (PDPC) is mandated with such function[5]. In the Philippines, there are no rules prohibiting transfer of data outside the country but the data processing agreement with the destination country could be required.[6] As a result, each jurisdiction employs different standards on adequate privacy protections. The lack of harmonized practices creates hurdles for intra-regional data transfers and protection of data privacy.

At the regional level, there have been initiatives to harmonize rules on cross-border data transfers but they have not been concrete enough to render effective protection. The existing framework is under the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules, which allows transfers of personal data between APEC members. Unlike the GDPR, this framework is entirely voluntary. The region is also negotiating a new expansive trade agreement called the Regional Comprehensive Economic Partnership (RCEP) with more partners including China, Japan, Korea, Australia, New Zealand and India. RCEP is expected to establish a harmonized rule on data privacy. While the negotiation is on-going and kept confidential, the leaked working draft on an e-commerce chapter reveals that RCEP will include rules on cooperation, trade facilitation (paperless trading, electronic signature certification), online consumer protection, personal data protection, and cross-border data transfers and prevention of data localization.

---

[2] Singapore: the Personal Data Protection Act 2012 (No. 26 of 2012); Malaysia: the Personal Data Protection Act 2010 (PDPA); The Philippines: the Data Privacy Act of 2012 (Republic Act No. 10173); Indonesia: regulation concerning provisions of electronic systems and transactions (Reg. 82) and Ministry of Communications & Informatics regarding the protection of personal data in an electronic system (MOCI Regulation); Vietnam: the Civil Code of Vietnam (No. 91/2015/QH13); Law on Information Technology (No. 67/2006/QH11); Law on Network Information Security (No. 86/2015/QH13); Law on E-Transactions (No. 51/2005/QH11); Law on Consumer Protection (No. 59/2010/QH12) and Decree No. 52/2013/ND-CP on e-commerce.

[3] Section 129 (1) and (2) of the Malaysia's Personal Data Protection Act 2010; Section 26 (1) and (2) of the Singapore's Personal Data Protection Act 2012.

[4] Section 129 (2) of the Malaysia's Personal Data Protection Act 2010.

[5] Section 26 (2) of the Singapore's Personal Data Protection Act 2012.

[6] Section 21 of the Data Privacy Act of 2012 (Republic Act No. 10173).

ASEAN is also developing an ASEAN Agreement on E-Commerce (expected to be concluded within 2018) to facilitate cross-border e-commerce transactions in ASEAN.[7] It is expected that cross-border privacy will be an important issue to be negotiated under the Agreement. At the same time, a few countries in the region are also negotiating the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), which is based on the Trans-Pacific Partnership (TPP) negotiation minus the United States. The CPTPP privacy rules are expected develop from the former TPP electronic commerce chapter (Chapter 14) to allow cross-border transfers of personal information when the transfers are related to conduct of business by members. In TPP chapter 14, restrictions to cross-border data transfers can only be imposed on legitimate public policy grounds, and must not be applied arbitrarily, or by means that create unjustifiable discrimination or a disguised restriction on trade.[8]

Countries in Southeast Asia with data privacy regulations in place use different institutional approaches in protecting cross-border personal data. Many countries in the region do not even have privacy regulations in place. Also, countries that join different international or regional frameworks will have different approaches in regulating cross-border privacy. This create obstacles for cross-border data transfers within the region. A country with high level of privacy standards could restrict transfers of data to a county that does not have adequate data protection regulation. As a result, there are lock-in benefits for countries that recognize privacy standards of one another as countries with different or less protection standards could be left out.

The paper will analyze texts of existing cross-border privacy regulations in Southeast Asian countries and international frameworks (CPTPP, APEC, and under-negotiating RCEP) focusing on different models of institutional enforcement to protect cross-border privacy. The paper will compare existing institutional enforcement models in Southeast Asia with those of GDPR to analyze whether there are possibilities to create a harmonized rule to streamline cross-border privacy rules across Southeast Asian region. The paper will propose a streamlined institutional approach for cross-border data transfers in Southeast Asia in order to facilitate international trade and afford cross-border data protection in the region.

2. ARGUMENTS FOR FREE FLOW OF CROSS-BORDER DATA

Free flow of cross-border data is important for a creation of a data-driven innovation. Industries are driven by adoption of technologies (i.e. data analytics and cloud computing) to increase efficiency in a number of areas such as monitoring productivity, managing workforce and supply chain, and support real-time services.[9] These industries collect and analyze personal data to better understand customer's behavior and to adapt their business accordingly.[10] There is a recent study by McKinsey that data flows have increased GDP worldwide by 10.1 percent over the past

[7] UNCTAD, 'Towards an ASEAN Agreement on E-commerce' Geneva, Switzerland (17 April 2018) <http://unctad.org/en/pages/MeetingDetails.aspx?meetingid=1730>. Accessed 18 June 2018.
[8] Art. 14.11 (1) and (2) of the CPTPP.
[9] Daniel Castro and Alan McQuinn, 'Cross-Border Data Flows Enable Growth in All Industries' Information Technology and Innovation Foundation (February 2015) <http://www2.itif.org/2015-crossborder-data-flows.pdf>. Accessed 12 July 2018.
[10] National Board of Trade Sweden, 'No Transfer, No Trade—the Importance of Cross-Border Data Transfers for Companies Based in Sweden' Stockholm, Sweden: National Board of Trade Sweden (January 2014).

decade.[11] In the United States, digitally-enabled services grew from $282.1 billion in 2007 to $356.1 billion in 2011.[12]

While benefits of international trade can be gained by allowing free flows of cross-border data, there can be arguments against allowing free flow of data across jurisdictions. The main reason is that free flow of cross-border data poses challenges to data privacy.[13] Insufficient protection of data privacy can create negative market effect by reducing consumers' confidence.[14] Jurisdictions like the EU consider the protection of personal data as a fundamental right[15] while many others prescribe the protection of individual privacy in constitutional doctrines or in civil codes.[16] Certain countries impose blanket restrictions on cross-border data transfers while some others only restrict data transfers on specific sectors such as personal, health, accounting, tax, gambling, financial, mapping, government, telecommunications, e-commerce, and online publishing data.[17]

There is a fine line between protecting a personal data and creating unnecessary barriers to the flow of data.[18] A heavy restrictions on cross-border data transfers can limit a growth of innovation.[19] An array of restrictions is implemented because of the fear that the destination country does not have an adequate or similar standard of personal data protection as the exporting country. In addition, a call for restrictions of cross-border data transfer is intensified when the majority of personal data is sensitive data of individuals such as health, finance, preferences and other personal data.[20] Many countries use impact assessment and offer strong data security standards, user awareness, and data portability.[21]

Another reason is some countries believe retaining data within their territories will create an opportunity for high-tech economic activity to take place within their borders.[22] This is a concept

[11] James Manyika and others, 'Digital Globalization: The New Era of Global Flows' McKinsey Global Institute (February 2016) <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-thenew-era-of-global-flows>. Accessed 12 July 2018.
[12] United States International Trade Commission, 'Digital Trade in the U.S. and Global Economies, Part 2' Publication Number: 4485 (August 2014) <https://www.usitc.gov/publications/332/pub4485.pdf>. Accessed 12 July 2018.
[13] US - ASEAN Business Council, 'Enabling Cross-Border E-Commerce Trade in ASEAN ' Washington (2016) <https://chambermaster.blob.core.windows.net/userfiles/UserFiles/chambers/9078/File/USABCe-CommercePaperFINAL.pdf>, 18. Accessed 12 July 2018.
[14] UNCTAD, *Data protection regulations and international data flows: Implications for trade and development* (United Nations, 2016), xi.
[15] Preamble (1) of the GDPR.
[16] See N. 14 above, UNCTAD, xi.
[17] Nigel Cory, 'Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? ' Information Technology and Innovation Foundation (2017) <https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>, 20. Accessed 12 July 2018.
[18] APEC, 'The Cross Border Privacy Rules System: Promoting consumer privacy and economic growth across the APEC region' (5 September 2013) <https://www.apec.org/Press/Features/2013/0903_cbpr.aspx>. Accessed 16 May 2018.
[19] See N. 13 above, US – ASEAN Business Council, 18.
[20] Jeffrey L. Bleich and Grant A. Davis-Denny, 'The Latest Cross-Border Privacy Rules In Asia-Pacific' (2015) <https://m.mto.com/Templates/media/files/Reprints/Law360_The%20Latest%20Cross-Border%20Privacy%20Rules%20In%20Asia-Pacific.pdf>, 1. Accessed 21 June 2018.
[21] See N. 13 above, US – ASEAN Business Council, 18.
[22] See N. 17 above, Cory, 5.

normally known as "data localization" in which a country enact law or policy requiring a company to store and process data locally, prohibition of oversea sharing of data, and mandating individual or government consent for data transfers.[23] Implementation of a data localization policy is argued to represent barriers to digital trade.[24] A 2014 International Trade Commission (ITC) estimated that removing foreign digital trade barriers would increase the United States GDP by $16.7 to $41.4 billion (0.1 to 0.3 percent) and wages by 0.7 to 1.4 percent in the seven digitally intensive sectors.[25]

There is a study in 2017 indicating that implementing data localization policy and other forms of cross-border data flow restrictions would reduce U.S. GDP by 0.1-0.36 percent, causing a price increase in certain cloud services in Brazil and the European Union by 10.5 to 54 percent, and reducing GDP in Brazil, China, the European Union, India, Indonesia, Korea, and Vietnam by 0.7-1.7 percent.[26] At a firm level, implementing data localization makes firms less competitive since companies incur more costs than necessary on IT services such as creating data storage and data center. This creates more burden for small economies which are not normally home to a data center.[27] Moreover, there are more compliance costs on data localization such as engaging data protection officers and procuring services to get individual and government consent to transfer data.[28]

There is a development gap among countries in Southeast Asia. Moreover, only a few counties in the region have a comprehensive data privacy regulation in place. As cross-border data flows are vital to business, an alignment of cross-border data privacy standards in the region will lead to economic gains from an exchange of information and a data-driven innovation. Harmonizing data privacy policies between countries in the region become a key factor to a development of international trade.

3. SOUTHEAST ASIAN FRAMEWORKS IN CROSS-BORDER DATA TRANSFERS

3.1 Asia-Pacific Economic Cooperation (APEC)

The APEC is a common standard of privacy throughout APEC members.[29] The APEC adopted the Cross-Border Privacy Rules (CBPR) which use a voluntary certification system for complying with APEC's privacy framework. Participation in the CBPR is voluntary for both APEC members and for companies within those countries.[30] Countries that take part in the CBPR scheme must designate an accountability agent and a privacy enforcement authority.[31] The accountability agent

[23] Ibid, 2.
[24] Ibid, 5.
[25] Ibid.
[26] Ibid, 2.
[27] Ibid, 6.
[28] Ibid, 7.
[29] Currently 21 countries are APEC members: Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong, China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, The Philippines, The Russian Federation, Singapore, Chinese Taipei, Thailand, United States of America, and Viet Nam.
[30] See N. 20 above, Bleich and Davis-Denny, 4.
[31] Ibid, 4.

is responsible for assessing and certifying a company's compliance with APEC privacy framework. Only firms based in the country of the accountability agent (can be foreign or domestic subsidiaries) are eligible for certification by that of accountability agent.[32] Businesses may adopt the CBPR principles and policies and then seek accreditation from the accountability agent.[33] In August 2013, IBM was the first US Company to be certified under the CBPR) system. TRUSTe, the accountability agent from US, approved IBM's compliance with APEC data protection standards. In 2016, JIPDEC, the accountability agent from Japan, became the second agent to be certified. [34] There is the APEC capacity building project that helps economies select an accountability agent to certify companies or provides other assistance to facilitate a member's readiness to adopt the Cross-Border Privacy Rules system.[35]

The privacy enforcement authority must be able to take enforcement action if a certified firm breaches its own certified privacy policies.[36] The privacy enforcement authorities from APEC members may work together to assist in data privacy-related investigations or enforcement matters through their participation in the APEC Cross-Border Privacy Enforcement Arrangement (CPEA).[37] However, the CBPR only applies to data controller and not data processor, although APEC is creating a separate but similar system called Privacy Recognition for Processors.[38]

The main problem is only a few countries are participating in the CBPR scheme (USA, Japan, Mexico, Canada, Korea, and Singapore). With a low participation level, it is unlikely that a country would prioritize joining the CBPR scheme. In addition, having a CBPR certification does not establish compliance with domestic law of APEC member countries that do not join the CBPR scheme. Countries like Australia does not regard a CBPR certification as "binding scheme" that is substantially similar to domestic privacy principles.[39]

3.2 Regional Comprehensive Economic Partnership (RCEP)

There are 16 countries taking part in negotiating the RECP (10 ASEAN member states and China, Japan, Korea, Australia, New Zealand and India). The RCEP would cover issues that are critical to the digital economy such as custom duties on electronic products, supply of cross-border services, paperless trading, telecommunications, intellectual property, source code disclosure, privacy and cross-border data flows.[40] As the text of the agreement is secretive, there is a proposal by the Asian Trade Center in June 2016 calling for a free movement of information across the Internet, including the free transfer or access to electronic information, except where necessary to achieve a legitimate public policy objectives such as data protection. The proposal also calls for a prohibition of any requirement concerning data localization including a requirement to use or locate computing facilities within a country as a condition for doing business in that country.

---

[32] Ibid, 4.
[33] See N. 14 above, UNCTAD, 4.
[34] See N. 18 above, APEC.
[35] Ibid.
[36] See N. 20 above, Bleich and Davis-Denny, 4.
[37] See N. 18 above, APEC.
[38] See N. 20 above, Bleich and Davis-Denny, 4.
[39] Ibid.
[40] Jyoti Panday, 'The Post-TPP Future of Digital Trade in Asia' (*Electronic Frontier Foundation*, 2 March 2018) <https://www.eff.org/deeplinks/2018/02/rcep-negotiations-face-obstacles-member-nations-unwilling-commit>

3.3 Comprehensive and Progressive Trans-Pacific Partnership (CPTPP)

The CPTPP, also known as TPP 11 is a singed trade agreement between Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam. The negotiated agreement texts are based on the previously-negotiated TPP. The CPTPP's electronic commerce chapter (based on the TPP's electronic commerce chapter) will set rules on the region including free flow of electronic data, access to software soft code, rules applicable to domain name, privacy and dispute resolution.[41]

In cross-border data transfers, the CPTPP recognizes each member's own privacy regulation on transfers of data but mandates members to allow cross-border transfer of information by electronic means, including personal information when this activity is for the conduct of business.[42] The restrictions of cross-border data transfers are allowed under a legitimate public policy reason but such restrictions on transfers must not cause an arbitrary or unjustifiable discrimination or a disguised restrictions on trade, and must not impose such restrictions on transfers greater than are required to achieve the legitimate public policy.[43]

The CPTPP sets a cooperation scheme for members to work together in exchanging information and share experiences on regulation, enforcement and compliance regarding personal information protection, online consumer protection, unsolicited commercial electronic messages, security in electronic communications, authentication, e-government, and also encourage setting up methods of self-regulation including codes of conduct, model contracts, guidelines and enforcement mechanism.[44] However, this cooperation scheme only impose a soft obligation or recommended measures to members.

3.4 A Proposed ASEAN Agreement on E-Commerce

The Agreement is being negotiated and to be concluded by the end of 2018. It is expected to streamline regional trade rules governing e-commerce to promote greater digital connectivity and lower operating barriers to entry for businesses. This will enhance the regional trade architecture for e-commerce, realize freer movement of e-commerce goods across Southeast Asia and support the regional expansion of companies based in ASEAN.[45] The objectives of the Agreement are to facilitate cross-border e-commerce transactions, contribute to creating an environment of trust and confidence in the use of e-commerce, and deepen cooperation among ASEAN Member States to

[41] Ibid.
[42] Art. 14.11 (1) and (2) of the CPTPP.
[43] Art. 14.11 (3) of the CPTPP.
[44] Art. 14.15 of the CPTPP.
[45] Ministry of Trade and Industry Singapore, 'Factsheet, ASEAN Agreement on Electronic Commerce' (1 March 2018) <https://www.mti.gov.sg/MTIInsights/SiteAssets/Pages/COS%202018/Factsheets/Support%20for%20Internationalisation%20and%20Innovation/ASEAN%20Agreement%20on%20Ecommerce%20MTI%20COS%202018%20Factsheet%20-%20final.pdf>. Accessed 12 June 2018.

further develop and intensify the use of e-commerce to drive economic growth and social development in the region.[46]

4. REGULATION OF CROSS-BORDER DATA TRANSFERS BY COUNTRY

4.1 Singapore

The Personal Data Protection Act 2012 (No. 26 of 2012) prohibits transfers of data outside Singapore unless the destination organization provides assurance that it will comply with Singaporean privacy standards.[47] The law explains mechanisms to achieve this. The destination organization is subject to legal obligations (contract, data transfer agreements, binding rules) that are comparable to the protection provided by Singaporean Law. Singapore data owner can consent to have their data transferred overseas.[48] The cross-border data transfers are allowed if the transfers are deemed necessary for the performance of contract between the organization and the individual, subject to certain conditions being met.[49]

Singapore's Personal Data Protection Commission (PDPC) issued a guidance for organizations on cross-border transfer including model clauses for data transfer agreements, and also published a new guide to data sharing (covering intra group and third party sharing).[50] In terms of enforcement, the Singapore's PDPC published the Advisory Guidelines on Enforcement of Data Protection Provisions in April 2016. The guidelines explain details on how the Commission should handle complaints, reviews and investigations of breaches of the data protection rules under the Act, and how to reach enforcement and sanctions. These guidelines also establish Commission's enforcement objectives, and guidance regarding the mitigating and aggravating factors that the Commission will take into account when issuing directions and sanctions (for example, prompt initial response and resolution of incidents; co-operation with investigations; and breach notification). Decisions or reconsiderations of the Commission may also be appealed to a Data Protection Appeal Committee.[51]

4.2 Indonesia

A new draft Bill on the Protection of Private Personal Data is being discussed but has not been enacted. However, there is regulation concerning provisions of electronic systems and transactions (Reg. 82) and Ministry of Communications & Informatics regarding the protection of personal data in an electronic system (MOCI Regulation) which require overseas transfers of personal data that are managed by an electronic system operator to coordinate and report details of transfers to

[46] Ibid.
[47] Section 26 (1) of the Singapore's Personal Data Protection Act 2012.
[48] See N. 20 above, Bleich and Davis-Denny, 3.
[49] DLA Piper, 'Data Protection Laws of the World: Singapore' (25 Jan 2018) <https://www.dlapiperdataprotection.com/index.html?t=transfer&c=SG>. Accessed 18 June 2018.
[50] Ibid.
[51] Ibid.

MOCI and implement laws concerning the cross-border exchange of data.[52] In terms of enforcement, an authority can impose a fine and imprisonment for breaches of data privacy and failing to comply with MOCI regulation. An authority can use a number of tools to force compliance such as a verbal and written warning including a temporary dismissal of activities or an announcement on website.[53]

Indonesia has a separate data privacy regulation in a banking sector. Overseas transfers of bank customer data in Indonesia must obtained an approval from the Bank of Indonesia (Bank Indonesia's Regulation No. 9/15/PBI/2007 on the Implementation of Risk Management in the Utilisation of Information Technology by the Bank).[54]

4.3 Malaysia

The Personal Data Protection Act 2010 (PDPA) does not permit cross-border data transfers unless the destination country has been approved to have an adequate level of protection comparable to the Malaysian law by the Minister of Information, Culture and Communications.[55] In 2017, a draft Personal Data Protection (Transfer of Personal Data to Places Outside Malaysia) has been passed to obtain feedbacks on the proposed jurisdictions to which personal data from Malaysia may be transferred.[56] As of 12 January 2018, the Minister has yet to approve any jurisdiction in which cross-border data transfer from Malaysia is allowed.

Regardless of passing the adequacy test, cross-border data transfers can be permitted if the data subject gives consent to such transfer, or if the transfer is necessary for the performance of the contract, or if the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights, or if the data user has taken all reasonable steps and exercised all due diligence to ensure that the processing of personal data would not contravene with PDPA, or if the transfer is necessary to protect the vital interest of the data subject.[57] In terms of enforcement, a violation of the PDPA incurs criminal liability. The prescribed penalties include pressing of fines and imprisonment. Directors, CEOs, managers or

[52] Article 22 (1) of the Minister of Communications & Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System (MOCI Regulation) states that transferring Personal Data that is managed by an electronic system operator at the government and regional government institution including the public or private sector domiciled in the territory of Indonesia to parties outside the territory of Indonesia must: (1) coordinate with the MOCI or the official or institution being authorized for such purpose; and (2) implement the laws and regulations regarding the transboundary exchange of Personal Data.
The implementation of the coordination as stipulated in Article 22 (1) of MOCI Regulation are: (1) to report the implementation plan of Personal Data transfer, at least containing the clear name, designated country, recipient subject name, implementation date, and reason/purpose of the transfer; (2) to request for advocacy, if needed; and (3) to report the activities implementation result.
[53] DLA Piper, 'Data Protection Laws of the World: Indonesia: Enfocerment' (25 Jan 2018) <https://www.dlapiperdataprotection.com/index.html?t=enforcement&c=ID>. Accessed 18 June 2018.
[54] Ibid.
[55] Section 129 (1) and (2) of the Malaysia's Personal Data Protection Act 2010.
[56] DLA Piper, 'Data Protection Laws of the World: Malaysia: Transfers' (25 Jan 2018) <https://www.dlapiperdataprotection.com/index.html?t=transfer&c=MY>. Accessed 18 June 2018.
[57] Section 129 (3) of the Malaysia's Personal Data Protection Act 2010.

other similar officers will have joint and several liability for non-compliance, subject to a due diligence defence.[58]

4.4 The Philippines

The Data Privacy Act of 2012 (Republic Act No. 10173) established the National Privacy Commission to monitor security breaches and issue guidelines concerning a security policy.[59] Cross-border transfers of personal information are allowed but the personal information controller is responsible for any occurrence to the personal information under its control subject to cross-border arrangement and cooperation.[60] However, the transfer, of sensitive personal information[61] to third parties, whether domestically or internationally, is prohibited. In terms of enforcement, criminal and monetary penalties are imposed for a failure to comply with the law.[62]

4.5 Thailand

At the moment, the draft Personal Information Protection Act is under reviewed. It provides protection of personal data by restricting the gathering, using, disclosing and altering of any personal data without the consent of the data owner. The Draft also imposes both criminal penalties and civil liability for any violation of the Draft and calls for the establishment of a Protection of Personal Data Commission to regulate compliance with the Draft.[63]

4.6 Vietnam

There is no single comprehensive data privacy regulation in Vietnam. In cross-border data transfers, individuals and organizations are allowed to transfer personal information outside Vietnam provided that prior consent from the data subject has been obtained.[64] In transferring the sensitive data such as information in banking sector, the person making the transfer must encrypt

---

[58] Sections 131-133 of the Malaysia's Personal Data Protection Act 2010.
[59] Chapter II of the Data Privacy Act of 2012 (Republic Act No. 10173).
[60] Section 21 of the Data Privacy Act of 2012 (Republic Act No. 10173).
[61] Sensitive Personal Information is defined by the Data Privacy Act of 2012 in Section 1 (i) as:
(1) personal information about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations, an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offence committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings.
(2) personal information issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or cm-rent health records, licences or its denials, suspension or revocation, and tax returns, and specifically established by an executive order or an act of Congress to be kept classified.
[62] Chapter VIII of of the Data Privacy Act of 2012 (Republic Act No. 10173).
[63] DLA Piper, 'Data Protection Laws of the World: Thailand' (25 Jan 2018) <https://www.dlapiperdataprotection.com/index.html?t=law&c=TH>. Accessed 18 June 2018.
[64] Art 38 (2) of the Civil Code of Vietnam (No. 91/2015/QH13); Article 21 (1) of Law on Information Technology (No. 67/2006/QH11); Article 17 (1) of Law on Network Information Security (No. 86/2015/QH13) Art 17(1)Bleich and Davis-Denny ; Art 46 (2) of Law on E-Transactions (No. 51/2005/QH11); Art 6 (2) ibid. of Law on Consumer Protection (No. 59/2010/QH12) and Art. 70 (1) of Decree No. 52/2013/ND-CP on e-commerce.

the information before transferring, in addition to obtaining a consent from the data subject.[65] Also, cross-border transfers of banking data require a written agreement specifying responsibilities of the parties involved, including terms and conditions, consequences of breaches and liability to pay compensation for loss and damages arising from such breach.[66]

The Ministry of Information and Communications (MIC) has the power to examine, inspect, settle complaints and denunciations, and handle data privacy violations in relation to the telecom, Internet and information technology sectors.[67] The Vietnam e-Commerce and Information Technology Authority (VECITA) under the Ministry of Industry and Trade has the power to handle data privacy violations in relation to the e-commerce sectors, including guiding, licensing, monitoring and controlling the operation of e-commerce activities in Vietnam.[68] There is no requirement on the comparable standards in which the data export needs to ensure that the recipient is legally bound to handle or process data under comparable privacy measures or under binding contracts, except for transfer of banking data mentioned above.[69]

5. APPROACHES IN PERMITTING CROSS-BORDER DATA TRNASFERS

While countries in the region have different regulatory and institutional approaches in data privacy, there are certain common approaches in permitting cross-border data transfers. The first approach is the permission for cross-border data transfers when there are "circumstantial exceptions" that require for such transfers to take place for the following reasons: (1) the transfer is necessary for the performance of a contract between the data subject and the controller or between the controller and a third party, (2) the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights, (3) the transfer is necessary in order to protect vital interests of the data subject. These circumstantial exceptions are used by Singapore and Malaysia.

The second approach is permission of cross-border data transfer when the destination country is approved by the authority of the exporting country to have "adequacy" of protection standards for personal data. This approach is stipulated in Malaysia's PDPA but the authority has not proposed a list of countries that pass the adequacy requirement so far.

The third approach is the "binding rules" mechanism. In this approach, the destination organization establishes review process and mechanisms that provide a sufficient degree of personal data protection (typically within an affiliated corporate group). Singapore uses this approach.

---

[65] Art. 16 of Decree No. 33/2002/ND-CP on detailing the implementation of the Ordinance on the protection of state secrets and Arts. 21 (2) and 35 (2) of Circular No 31/2015/TT-NHNN regulating safety and confidentiality of banking information technology systems.

[66] Art. 30 (2) of Circular No. 31/2015/TT-NHNN regulating safety and confidentiality of banking information technology systems (Circular 31)

[67] Art. 9 (2) (dd) of Law on Telecommunications; Art. 10 (1) of Law on Information Technology (No. 67/2006/QH11); Art. 39 (1) Bleich and Davis-Denny of Decree No. 72/2013/ND-CP on management, provision and use of Internet services and online information; Art. 27 (2) ibid. of Law on Network Information Security (No. 86/2015/QH13).

[68] Arts. 6 (1), 77 and 78 (5) of Decree No. 52/2013/ND-CP on e-commerce.

[69] Waewpen Piemwichai, *Jurisdictional Report: Socialist Republic of Vietnam* in Asian Business Law Institute (ed), *Regulation of Cross-border Transfers of Personal Data in Asia, A compendium of 14 reports by the Asian Business Law Institute* (2018), 406.

The fourth approach is assessing whether legal obligations in the "contracts" between the exporting organization and the destination organization provide a sufficient degree of protection for the transfer of personal data. This approach is used by Singapore, the Philippines, and Vietnam (only in a banking sector).

The other approach is to examine whether the data subject gives "consent" to the transfer of their data overseas. This approach is employed by Singapore, Malaysia, and Vietnam.

Table 1: Approaches in permitting cross-border data transfers in Southeast Asian countries

Country	**Regulation Type**	**Permission of Cross-Border Data Transfers**	**Regulator**
Singapore	Comprehensive	Consent, binding rules, contracts, circumstantial exceptions	Personal Data Protection Commission
Indonesia	Draft of comprehensive law being discussed	Report to regulator (in banking sector only, report to Bank of Indonesia)	Ministry of Communication and Informatics
Malaysia	Comprehensive	Consent, adequacy (yet to have adequacy list), circumstantial exceptions	Ministry of Information, Culture and Communication
Philippines	Comprehensive	Contracts (place liability to data controller) Prohibit transfers of sensitive data	National Privacy Commission
Vietnam	Multiple (e.g. civil codes, information law, e-commerce law)	Consent (contracts and consent in Banking sector only)	Ministry of Information and Communication
Other countries in the region (Myanmar, Thailand, Lao, Cambodia, and Brunei) either have no data privacy regulation or on the process of developing one.			

There are approaches in other countries outside Southeast Asia worth mentioning. The European Union's General Data Protection Regulation (GDPR) in 2016 harmonizes data privacy regulation within the EU and accord free flow of data transfers within the EU, but only allow data transfers to non-EU countries if destination countries have adequate data protections. In Australia, a firm that transfers personal data oversee to a foreign business must ensure that the foreign business does not breach "APPs" (13 Privacy Principles). Generally, this can be done via a contractual agreement requiring an oversee recipient to handle personal information in accordance with APPs. Exceptions of making a contract are (1) the recipient has adequate protection (e.g. it binds itself to "binding rules"), or (2) an Australian firm receives consent from a customer that is willing to pass information onto a foreign provider that does not have privacy controls.[70] However, Australia has more restrictive regulation for medical records which are not permitted to be transferred overseas.

[70] See N. 20 above, Bleich and Davis-Denny, 2.

In New Zealand, the approach is unique in the sense that it prohibits data imported into New Zealand to be exported outside New Zealand if (1) the destination country lacks adequate protection comparable to the laws of New Zealand, and (2) the transfer would contravene with OECD's privacy rules. This is to prevent, for example, the EU using New Zealand (which is already passed EU adequacy test) as a conduit to transfer to another country.[71] In Hong Kong, the 2014 guidance of Hong Kong's Privacy Commissioner limits the transfer of data outside Hong Kong except for limited circumstances. These exceptions include countries that have been approved by Hong Kong Privacy Commissioner, countries that have reasonable grounds for believing that have laws similar to or serve the same purpose as Hong Kong, or have agreements to ensure the data will be protected in accordance with Hong Kong's privacy standards.[72]

Table 2: Approaches on cross-border data transfers and data localization in other countries

Country	Rules on Cross-Border Data Transfers and Data Localization
Argentina	- Overseas data transfers are allowed if destination countries have adequate data protections (but has permitted any country so far as of 2017), or the data subject gives explicit consent.[73] - Cloud storage is considered cross-border transfer of data (National Directorate for Personal Data Protection issued Provision no. 18/2015).
Australia	- Overseas data transfers are allowed via contractual agreements ensuring compliance with Australia's privacy principles unless the data subject consents to such transfer, or the destination country has an adequate level of protection - Personal health records to be stored only in Australia.[74]
Belgium	- Accounting and tax records to be kept at premises of the taxpayer. - The accounting records can be kept overseas provided that immediate access can be granted on short notice.[75]
Brazil	Forced data localization for public procurement contracts involving cloud-computing services.[76]
Bulgaria	- A gaming license holder to store all data related to operations in Bulgaria locally. - The company's communication equipment and central control point for IT must be in Bulgaria, another EU member country, or Switzerland.[77]
Canada	- Two Canadian provinces, British Columbia and Nova Scotia, require personal data to be held by public bodies and must be stored and accessed only in Canada unless certain conditions are fulfilled.[78]

[71] Ibid, 3.
[72] Ibid.
[73] Estudio Beccar Varela et al., 'Data Protection in Argentina: Overview' Practical Law: A Thomson Reuters Legal Solution <http://uk.practicallaw.com/3-586-5566>. Acessed 21 July 2018.
[74] Personally Controlled Electronic Health Records Act 2012, no. 63, Australia (2012). <https://www.legislation.gov.au/Details/C2012A00063>. Accessed 21 July 2018.
[75] EU Country Guide Data Localization & Access Restriction: De Brauw Blackstone Westbroek, January 2013 (2013) <http://www.verwal.net/wp/wp-content/uploads/2014/03/EU-Country-Guide-Data-Locationand-Access-Restrictions.pdf>. Accessed 21 July 2018.
[76] Paulo Trevisani and Loretta Chao, 'Brazil Lawmakers Remove Controversial Provision in Internet Bill' The Wall Street Journal (2014) <https://www.wsj.com/articles/SB10001424052702304026304579449730185773914>
[77] Gambling Act, Bulgaria (2012), <http://www.dkh.minfin.bg/document/403>. Accessed 21 July 2018.
[78] Anupam Chander and Uyen P. Le, *Data Nationalism*, 64 *Emory Law Journal* (2015)

Country	Rules on Cross-Border Data Transfers and Data Localization
	- The tender for the government ICT project in 63 agencies requires storage of data in Canada (for national security reasons).[79]
China	- Prohibiting overseas data transfers if it brings risks to the security of the national political system, economy, science and technology, or national defense.[80] - In 2006, e-banking companies to keep their servers in China.[81] - In 2011, prohibition of the off shore analyzing, processing, or storage of Chinese personal financial information.[82] - In 2013, all credit information on Chinese citizens to be processed and stored in China.[83] - In 2014, health and medical information to be stored in China.[84] - In 2015, draft regulations for data localization of insurance industry.[85] - In 2016, internet-based mapping service to store data in China.[86] - In 2016, a broad range of services including online publishing, app stores, audio and video distribution platforms, online literature database, and online gaming to locate servers in China.[87] - In 2016, internet and telecommunication companies and other providers of "critical information infrastructure" to store data on Chinese servers and provide encryption key to the government and any action to transfer data overseas must undergo "security assessment".[88]

[79] United States Trade Representative, 'The 2017 National Trade Estimate report' (Washington, DC: United States Trade Representative (2017) <https://ustr.gov/sites/default/files/files/reports/2017/NTE/2017%20NTE.pdf>. Accessed 21 July 2018.

[80] Stephen J. Ezell, Robert D. Atkinson and Michelle A. Wein, 'Localization Barriers to Trade: Threat to the Global Innovation Economy ' Information Technology and Innovation Foundation (2013) <http://www2.itif.org/2013-localization-barriers-to-trade.pdf>. Accessed 21 July 2018.

[81] Timothy Stratford and Yan Luo, '3 Ways Cybersecurity Law in China Is About to Change' Law360, May 2, 2016 (2016) <https://www.law360.com/articles/791505/3-ways-cybersecurity-law-in-china-is-about-tochange>. Accessed 21 July 2018.

[82] People's Bank of China, 'Notice of the People's Bank of China on Urging Banking Financial Institutions to Do a Good Job in Protecting Personal Financial Information' (21 January 2011) <http://www.lawinfochina.com/display.aspx?lib=law&id=8837&CGid=>. Accessed 21 July 2018.

[83] Regulation on the Credit Reporting Industry, State Council 228th session, China (2013), <http://www.pbccrc.org.cn/crc/jgyhfw/201309/1ca0f775b50744cabaf83538288d77a9/files/e8a8bf080ed64f48914a652da1d8fdc3.pdf>. Accessed 21 July 2018.

[84] "Interpretation on Population Health Information Management Measures (Trial Implementation)," National Health and Family Planning Commission of the PRC, last updated June 15, 2014, <http://en.nhfpc.gov.cn/2014-06/15/c_46801_2.htm>. Accessed 21 July 2018.

[85] Michael Martina, 'Concern over China insurance rules ahead of talks with U.S.' Reuters (31 May 2016) <http://www.reuters.com/article/us-china-cyber-insurance-idUSKCN0YM0NN>. Accessed 21 July 2018.

[86] Ron Cheng, 'Latest Developments on China's Cybersecurity Regulation' Forbes (30 June 2016) <https://www.forbes.com/sites/roncheng/2016/06/30/latest-developments-on-chinas-cybersecurityregulation/#7658dc6c3165>. Accessed 21 July 2018.

[87] "Online Publishing Service Management Rules," China Copyright and Media website, <https://chinacopyrightandmedia.wordpress.com/2016/02/04/online-publishing-servicemanagement-rules/>. Accessed 12 June 2018.

[88] "Protecting Data Flows in the US-China Bilateral Investment Treaty" (AmCham China, April, 2015), <http://www.amchamchina.org/policy-advocacy/policy-spotlight/data-localization>. Accessed 21 January 2018.

Country	Rules on Cross-Border Data Transfers and Data Localization
	- In 2016, a cyber security requirement to store personal data and important business data in China.[89] - In 2016, a local data storage requirement for cloud computing services.[90] - In 2017, a draft regulation requiring extensive data localization on all network operators (which is likely any owner or administrator of a computerized network system).[91]
Colombia	- Ministry of Information and Communication Technology's recommendation for data localization of "basic digital services" and data processing center should be in Colombia.[92] - The National Procurement Office restricts cross-border data flows in cloud service procurement project for the government.[93] - Considering enacting rules of adequate data protections for overseas data transfers (reportedly preparing a list of "adequate" countries.[94]
Cyprus	Requiring certain categories of traffic and location data to be retained between 6 months and two years for a purpose of investigating, detecting, and prosecuting of serious crime and terrorism by the government.[95]
Denmark	- Data retention policy is still in force although the EU Directive on Data Retention was declared invalid by the European Court of Justice.[96] - In 2011, the Danish Data Protection Agency denied the City of Odense permission to transfer of data concerning health, serious social problems, and private matters to Google Apps for security reasons.[97] - The Book Keeping Act requires storage of accounting data in the country for 5 years except for special circumstances.[98]
European Union	- Allow overseas data transfers to non-EU countries if destination countries have adequate data protections.[99] - In 2017, EU has recognized 12 adequate countries so far: Andorra, Argentina, Canada, Switzerland, the Faeroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, the United States (through the U.S.-EU Privacy Shield Framework), and Uruguay.[100]

[89] Nigel Cory, 'The Worst Innovation Mercantilist Policies of 2016' Information Technology and Innovation Foundation (January 2017) <http://www2.itif.org/2017-worst-innovation-mercantilistpolicies.pdf>. Accessed 12 July 2018.
[90] Ibid.
[91] See N. 17 above, Cory, 22.
[92] Ibid.
[93] Ibid.
[94] Ibid.
[95] Matthias Bauer et al., 'Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States' European Centre for International Political Economy (March 2016) <http://ecipe.org//app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf>. Accessed 21 July 2018.
[96] Ibid.
[97] See N. 78 above, Chander and Le.
[98] See N. 75 above, EU Country Guide Data Localization & Access Restriction.
[99] European Commission, 'Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries' (24 November 2016) <http://ec.europa.eu/justice/dataprotection/international-transfers/adequacy/index_en.htm>. Accessed 21 July 2018.
[100] Ibid.

Country	Rules on Cross-Border Data Transfers and Data Localization
Finland	Accounting records to be stored in Finland or in another EU country if a real-time connection is guaranteed.[101]
France	- All data from public administration must be stored and processed in France.[102] - Prohibition of overseas data transfers for information involving legal proceedings.[103]
Germany	- Accounting data to be stored locally.[104] - Companies liable for German tax to keep accounting records in Germany (with some exceptions for multinational companies).[105]
Hong Kong	Overseas data transfers are only allowed if the destination country has adequate protections, or have agreements ensuring protections in accordance with Hong Kong's privacy standards.[106]
Greece	Data retention policy is still in force for data generated and stored on physical media although the EU Directive on Data Retention was declared invalid by the European Court of Justice.[107]
India	- Overseas data transfers are allowed only in two cases: when "necessary" and when the subject consents to transfer of data abroad.[108] - Data owned by the government or collected using public funds must be stored in local data centers.[109] - A requirement of data localization for all email providers to set up local servers.[110] - The 2015 National Telecommunication Machine-to-Machine Roadmap requires all gateway and application servers that serve customers in India to be located in India.[111] - Data localization for cloud providers computing for public contracts.[112]
Kazakhstan	- Data localization requirement for companies established in Kazakhstan (including branches and representatives of foreign companies) that use and collect personal data.

[101] See N. 17 above, Cory, 24.
[102] Ibid.
[103] Bertrand Liard, Caroline Lyannaz and David Strelzyk-Herzog, 'Discovery in the US Involving French Companies' White & Case (14 November 2012) <https://www.whitecase.com/publications/article/discovery-us-involving-french-companies>. Accessed 21 July 2018.
[104] See N. 17 above, Cory, 24.
[105] Ibid.
[106] See N. 20 above, Bleich and Davis-Denny, 3.
[107] Stavros Karageorgiou and Maria Mouzaki, 'Collection, Storage and Transfer of Data in Greece' Lexology (8 February 2017) <http://www.lexology.com/library/detail.aspx?g=58c33c75-7875-4444-80831887c19c1860>. Accessed 21 July 2018.
[108] See No. 78 above, Chander and Le.
[109] India's Department of Science and Technology, 'National Data Sharing and Accessibility Policy' (2012) <http://www.dst.gov.in/sites/default/files/nsdi_gazette_0.pdf>. Accessed 21 July 2018.
[110] Thomas K. Thomas, 'National Security Council Proposes 3-Pronged Plan to Protect Internet Users' The Hindu Business Line (13 February 2014) <http://www.thehindubusinessline.com/info-tech/nationalsecuritycouncil-proposes-3pronged-plan-to-protectinternet-users/article5685794.ece>. Accessed 21 July 2018.
[111] See N. 79 above, United States Trade Representative.
[112] Ibid.

Country	Rules on Cross-Border Data Transfers and Data Localization
	- It is uncertain whether this localization requirement applies to foreign companies without legal presence in Kazakhstan but whose websites are accessible in Kazakhstan.[113]
Luxembourg	- In 2012 circular by the financial services regulator, the financial institutions are required to process data in the country, unless the overseas entity is part of the same company or if there is an explicit consent for transfer of data.[114]
Nigeria	Data localization requirement for subscriber, government and consumer data.[115]
Russia	- Data operators who collect personal data about Russian citizen must "record, systematize, accumulate, store, amend, update and retrieve" data using databases physically located in Russia. These data can be transferred overseas but only after first stored in Russia.[116] - Companies to store actual contents of user's communications for six months (such as voice data, text messages, pictures, sounds, and video, not just the meta data).[117]
South Korea	- Overseas data transfers are allowed only when the data subject gives consent. In addition, the data subject must be informed of who receive data, recipient purpose of that information, period of information to be retained, and the specific personal information to be provided.[118] - Prohibiting mapping data to be stored outside the country.[119]
Taiwan	- Overseas data transfers are restricted in certain circumstances such as for national interests reasons, by treaty or agreement, inadequate protection at destination country, or when overseas transfer is used to avoid Taiwanese law.[120]

[113] Ravil Kassilgov, 'Kazakhstan—Localization of Personal Data' Lexology (12 January 2016) <http://www.lexology.com/library/detail.aspx?g=303621d9-e5b7-4115-9d8c-2a5d1d40ed2c>. Accessed 21 July 2018.

[114] "Joint Statement: Free Flow of Data"; "Circular CSSF 12/552 as amended by Circulars CSSF 13/563 and CSSF 14/597" (Luxemborg: Commission de Surveillance du Secteur Financier, December 11, 2012), <https://www.cssf.lu/fileadmin/files/Lois_reglements/Circulaires/Hors_blanchiment_terrorisme/cssf12_552eng_upd241114.pdf>. Accessed 23 February 2018.

[115] Nigerian Federal Ministry of Communication Technology, 'Guidelines for Nigerian Content Development in Information and Communication Technology' Nigeria: Nigerian Federal Ministry of Communication Technology (2014) <http://onc.org.ng/wp-content/uploads/2014/06/ONCFramework-2.pdf>. Accessed 21 July 2018.

[116] "Russia's Personal Data Localization Law Goes Into Effect" (Duane Morris, October 16, 2015), <http://www.duanemorris.com/alerts/russia_personal_data_localization_law_goes_into_effect_1015.html?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original>. Accessed 21 March 2018.

[117] Ksenia Koroleva, 'Yarovaya' Law—New Data Retention Obligations for Telecom Providers and Arrangers in Russia' Latham and Watkins Global Privacy and Security Compliance Law Blog (29 July 2016) <http://www.globalprivacyblog.com/privacy/yarovaya-law-new-data-retention-obligations-fortelecom-providers-and-arrangers-in-russia/>. Accessed 21 July 2018.

[118] Anupam Chandler and Uyen P. Le, *Breaking the Web: Data Localization vs. the Global Internet*, 40 *Emory Law Journal* (April 2014).

[119] Act on the Establishment, Management, etc. of Spatial Data (Korea: Ministry of Land, Infrastructure and Transport, June 3, 2014), <http://elaw.klri.re.kr/eng_service/lawView.do?hseq=32771&lang=ENG>. Accessed 16 March 2018.

[120] Personal Information Protection Act (promulgated by the Ministry of Justice, Taiwan, May 26, 2010), <http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021>. Accessed 2 April 2018. Accessed 21 July 2018.

Country	Rules on Cross-Border Data Transfers and Data Localization
Turkey	- Overseas data transfers are allowed when the data subject gives expressed consent. Also, the destination country must have an adequate level of data protection, unless the data protection board provides permission.[121]
United States	- Data localization requirement for federal tax information[122], and data concerning Department of Defense from cloud computing service provider.[123]

6. PROPOSED INSTITUTIONAL APPROACHES IN THE REGION

The main challenge in the region is fragmentation. Countries in the region accede to different instruments that have different principles in regulating cross-border data privacy. The APEC regime offers a wide range of memberships and flexibility in implementation but its CBPR regime, while being established for Asia-Pacific region including Southeast Asia, has only one participating country from Southeast Asia, which is Singapore. The rest of participating countries are limited also (only USA, Japan, Mexico, Canada, and Korea). Non-CBPR participating countries' own privacy laws will prevail over the CBPR. The trade agreements such as the RCEP and the CPTPP with wide memberships have potential to drive interoperability but it has a number of challenges. The negotiation is often complex and secretive which makes it burdensome to align domestic regulation in a timely manner. The institutional approach has complex cooperation procedures and dispute resolution mechanisms. The cooperation scheme is soft law obligations (e.g. exchange of information, enforcement cooperation, and investigation assistance), and members are not legally bound to comply with such obligations.

The other important challenge is a lack or non-existence of privacy regulation of developing countries in the region. Currently, only five out of ten countries in the region have data privacy regulation in place. Difficulties in developing the regulation is often associated with (1) the length of time it takes to pass legislation, (2) financial costs associated with implementing and enforcing a data protection regime, and (3) a lack of public and private sector knowledge and cooperation among governmental entities regulating in parallel.[124]

Jurisdictional restraints are main hurdles in managing cross-border personal data protection. A competent authority generally is unable to exercise an inquiry power overseas when a breach of personal data occurs outside its jurisdiction. Also, an enforcing authority such as a national court is unable to access an evidence or force any action when servers or cloud computing facility are established abroad. However, certain jurisdictions already adopt an extraterritorial approach to overcome these challenges. Japan added a new requirement in which if a data controller outside

[121] See N. 79 above, United States Trade Representative.
[122] Internal Revenue Service, 'Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies' Washington, DC: Internal Revenue Service (September 2016) <https://www.irs.gov/pub/irs-pdf/p1075.pdf>. Accessed 21 July 2018.
[123] "Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)" (Washington, DC: Defense Acquisition Regulations System, Department of Defense, August 26, 2015), <https://www.federalregister.gov/documents/2015/08/26/2015-20870/defense-federal-acquisitionregulation-supplement-network-penetration-reporting-and-contracting-for>. Accessed 21 April 2018.
[124] See N. 14 above, UNCTAD , xii.

Japan has collected personal information of Japanese citizens, that foreign data controller will be required to comply with key sanctions of the Japanese law.[125] In the EU, the GDPR will apply to the processing of personal data in the context of activities of controller or a processor in the EU, regardless of whether the processing takes place in the EU or not (Art. 3.1 of the GDPR). The GDPR will also apply to the processing of data subjects who are in the EU by a controller or processor not established in the EU if the processing activities relate to offering goods or services to data subjects in the EU or monitoring of behavior taking place in the EU (Art. 3.1 of the GDPR).

The paper proposes that there is a need for a unifying approach to regulate cross-border data transfer in the region to accommodate free flow of cross-border data transfers within the region while affording effective personal data protection. Since many countries in the region have already subscribed to different frameworks that mandate different schemes for cross-border data privacy protection, the new approach should not add more complexity by overriding them with a new mechanism. Creating a new mechanism would increase duplication and fragmentation in the regional approach. Rather than creating a new mechanism, the approach will recognize and supplement compatibility with different frameworks. The proposed ASEAN Agreement on E-Commerce, expected to be finalized by the end of 2018, should carry out this unifying function to promote interoperability. In principles, the new approach should include (1) an alignment with standards of APEC's CBPR rules, (2) a regional recognition scheme for "adequacy" test to verify that a particular country has a sufficient level of personal data protection, (3) a technical assistance to developing countries that have limited resources in data protection regulation, (4) a functioning body to provide regional guidelines and recommendation in which a designated data protection authority of a member country can communicate with one another and exchange ideas (5) an information sharing platform that includes exchange of information, research, experiences in data privacy protection, techniques in investigating data privacy violation, and regulation strategies and enforcement, (6) cross-border cooperation in investigation and enforcement that enables tools to notify another designated data protection authority when data privacy violation occurs and provide cross-border assistance in investigation and enforcement.

References

Anupam Chander and Uyen P. Le, 'Data Nationalism' (2015) 64 *Emory Law Journal*

Anupam Chandler and Uyen P. Le, 'Breaking the Web: Data Localization vs. the Global Internet' (April 2014) 40 *Emory Law Journal*

APEC, 'The Cross Border Privacy Rules System: Promoting consumer privacy and economic growth across the APEC region' (5 September 2013) <https://www.apec.org/Press/Features/2013/0903_cbpr.aspx>

Bertrand Liard, Caroline Lyannaz and David Strelzyk-Herzog, 'Discovery in the US Involving French Companies' White & Case (14 November 2012) <https://www.whitecase.com/publications/article/discovery-us-involving-french-companies>

[125] Ibid, 19.

Daniel Castro and Alan McQuinn, 'Cross-Border Data Flows Enable Growth in All Industries' Information Technology and Innovation Foundation (February 2015) <http://www2.itif.org/2015-crossborder-data-flows.pdf>

"Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018)" (Washington, DC: Defense Acquisition Regulations System, Department of Defense, August 26, 2015), <https://www.federalregister.gov/documents/2015/08/26/2015-20870/defense-federal-acquisitionregulation-supplement-network-penetration-reporting-and-contracting-for>.

DLA Piper, 'Data Protection Laws of the World' (25 Jan 2018) <https://www.dlapiperdataprotection.com>.

Estudio Beccar Varela et al., 'Data Protection in Argentina: Overview' Practical Law: A Thomson Reuters Legal Solution http://uk.practicallaw.com/3-586-5566>

EU Country Guide Data Localization & Access Restriction, De Brauw Blackstone Westbroek, January 2013 (2013) <http://www.verwal.net/wp/wp-content/uploads/2014/03/EU-Country-Guide-Data-Locationand-Access-Restrictions.pdf>

European Commission, 'Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries' (24 November 2016) <http://ec.europa.eu/justice/dataprotection/international-transfers/adequacy/index_en.htm>

India's Department of Science and Technology, 'National Data Sharing and Accessibility Policy' (2012) <http://www.dst.gov.in/sites/default/files/nsdi_gazette_0.pdf>

Internal Revenue Service, 'Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies' Washington, DC: Internal Revenue Service (September 2016) <https://www.irs.gov/pub/irs-pdf/p1075.pdf>

James Manyika and others, 'Digital Globalization: The New Era of Global Flows' McKinsey Global Institute (February 2016) <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-thenew-era-of-global-flows>

Jeffrey L. Bleich and Grant A. Davis-Denny, 'The Latest Cross-Border Privacy Rules In Asia-Pacific' (2015) <https://m.mto.com/Templates/media/files/Reprints/Law360_The%20Latest%20Cross-Border%20Privacy%20Rules%20In%20Asia-Pacific.pdf>

Jyoti Panday, 'The Post-TPP Future of Digital Trade in Asia' (*Electronic Frontier Foundation,* 2 March 2018) <https://www.eff.org/deeplinks/2018/02/rcep-negotiations-face-obstacles-member-nations-unwilling-commit>

Ksenia Koroleva, 'Yarovaya' Law—New Data Retention Obligations for Telecom Providers and Arrangers in Russia' Latham and Watkins Global Privacy and Security Compliance Law Blog (29 July 2016) <http://www.globalprivacyblog.com/privacy/yarovaya-law-new-data-retention-obligations-fortelecom-providers-and-arrangers-in-russia/>

Matthias Bauer et al., 'Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States' European Centre for International Political Economy (March 2016) <http://ecipe.org//app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf>

Michael Martina, 'Concern over China insurance rules ahead of talks with U.S.' Reuters (31 May 2016) <http://www.reuters.com/article/us-china-cyber-insurance-idUSKCN0YM0NN>

Ministry of Trade and Industry Singapore, 'Factsheet, ASEAN Agreement on Electronic Commerce' (1 March 2018) <https://www.mti.gov.sg/MTIInsights/SiteAssets/Pages/COS%202018/Factsheets/Support%20for%20Internationalisation%20and%20Innovation/ASEAN%20Agreement%20on%20Ecommerce%20MTI%20COS%202018%20Factsheet%20-%20final.pdf>

National Board of Trade Sweden, 'No Transfer, No Trade—the Importance of Cross-Border Data Transfers for Companies Based in Sweden' Stockholm, Sweden: National Board of Trade Sweden (January 2014) <

Nigel Cory, 'Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? ' Information Technology and Innovation Foundation (2017) <https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>

Nigel Cory, 'The Worst Innovation Mercantilist Policies of 2016' Information Technology and Innovation Foundation (January 2017) <http://www2.itif.org/2017-worst-innovation-mercantilistpolicies.pdf>

Nigerian Federal Ministry of Communication Technology, 'Guidelines for Nigerian Content Development in Information and Communication Technology' Nigeria: Nigerian Federal Ministry of Communication Technology (2014) <http://onc.org.ng/wp-content/uploads/2014/06/ONCFramework-2.pdf>

"Online Publishing Service Management Rules," China Copyright and Media website, <https://chinacopyrightandmedia.wordpress.com/2016/02/04/online-publishing-servicemanagement-rules/>.

Paulo Trevisani and Loretta Chao, 'Brazil Lawmakers Remove Controversial Provision in Internet Bill' The Wall Street Journal (2014) <https://www.wsj.com/articles/SB10001424052702304026304579449730185773914>

People's Bank of China, 'Notice of the People's Bank of China on Urging Banking Financial Institutions to Do a Good Job in Protecting Personal Financial Information' (21 January 2011) <http://www.lawinfochina.com/display.aspx?lib=law&id=8837&CGid=>

"Protecting Data Flows in the US-China Bilateral Investment Treaty" (AmCham China, April, 2015), <http://www.amchamchina.org/policy-advocacy/policy-spotlight/data-localization>.

Ravil Kassilgov, 'Kazakhstan—Localization of Personal Data' Lexology (12 January 2016) <http://www.lexology.com/library/detail.aspx?g=303621d9-e5b7-4115-9d8c-2a5d1d40ed2c>

Ron Cheng, 'Latest Developments on China's Cybersecurity Regulation' Forbes (30 June 2016) <https://www.forbes.com/sites/roncheng/2016/06/30/latest-developments-on-chinas-cybersecurityregulation/#7658dc6c3165>

"Russia's Personal Data Localization Law Goes Into Effect" (Duane Morris, October 16, 2015), <http://www.duanemorris.com/alerts/russia_personal_data_localization_law_goes_into_effect_1015.html? utm_source=Mondaq&utm_ medium=syndication&utm_campaign=View-Original>.

Stavros Karageorgiou and Maria Mouzaki, 'Collection, Storage and Transfer of Data in Greece' Lexology (8 February 2017) <http://www.lexology.com/library/detail.aspx?g=58c33c75-7875-4444-80831887c19c1860>

Stephen J. Ezell, Robert D. Atkinson and Michelle A. Wein, 'Localization Barriers to Trade: Threat to the Global Innovation Economy ' Information Technology and Innovation Foundation (2013) <http://www2.itif.org/2013-localization-barriers-to-trade.pdf>

Thomas K. Thomas, 'National Security Council Proposes 3-Pronged Plan to Protect Internet Users' The Hindu Business Line (13 February 2014) <http://www.thehindubusinessline.com/info-tech/nationalsecuritycouncil-proposes-3pronged-plan-to-protectinternet-users/article5685794.ece>

Timothy Stratford and Yan Luo, '3 Ways Cybersecurity Law in China Is About to Change' Law360, May 2, 2016 (2016) <https://www.law360.com/articles/791505/3-ways-cybersecurity-law-in-china-is-about-tochange>

UNCTAD, 'Towards an ASEAN Agreement on E-commerce' Geneva, Switzerland (17 April 2018) <http://unctad.org/en/pages/MeetingDetails.aspx?meetingid=1730>

UNCTAD, *Data protection regulations and international data flows: Implications for trade and development* (United Nations, 2016)

United States International Trade Commission, 'Digital Trade in the U.S. and Global Economies, Part 2' Publication Number: 4485 (August 2014) <https://www.usitc.gov/publications/332/pub4485.pdf>

United States Trade Representative, 'The 2017 National Trade Estimate report' (Washington, DC: United States Trade Representative (2017) <https://ustr.gov/sites/default/files/files/reports/2017/NTE/2017%20NTE.pdf>

US - ASEAN Business Council, 'Enabling Cross-Border E-Commerce Trade in ASEAN ' Washington (2016) <https://chambermaster.blob.core.windows.net/userfiles/UserFiles/chambers/9078/File/USABCe-CommercePaperFINAL.pdf>

Waewpen Piemwichai, 'Jurisdictional Report: Socialist Republic of Vietnam' in Asian Business Law Institute (ed), *Regulation of Cross-border Transfers of Personal Data in Asia, A compendium of 14 reports by the Asian Business Law Institute* (2018)

Legislation and cases

"Interpretation on Population Health Information Management Measures (Trial Implementation)," National Health and Family Planning Commission of the PRC, last updated June 15, 2014, http://en.nhfpc.gov.cn/2014-06/15/c_46801_2.htm.

"Joint Statement: Free Flow of Data"; "Circular CSSF 12/552 as amended by Circulars CSSF 13/563 and CSSF 14/597" (Luxemborg: Commission de Surveillance du Secteur Financier, December 11, 2012), <https://www.cssf.lu/fileadmin/files/Lois_reglements/Circulaires/Hors_blanchiment_terrorisme/cssf12_55 2eng_upd241114.pdf>.

Act on the Establishment, Management, etc. of Spatial Data (Korea: Ministry of Land, Infrastructure and Transport, June 3, 2014), <http://elaw.klri.re.kr/eng_service/lawView.do?hseq=32771&lang=ENG>.

Bank Indonesia's Regulation No. 9/15/PBI/2007 on the Implementation of Risk Management in the Utilisation of Information Technology by the Bank.

Case C-362/14. Maximillian Schrems v Data Protection Commissioner [2015] ECLI: EU:C:2015:650.

Circular No 31/2015/TT-NHNN regulating safety and confidentiality of banking information technology systems.
Decree No. 33/2002/ND-CP on detailing the implementation of the Ordinance on the protection of state secrets.
Decree No. 52/2013/ND-CP on e-commerce
Decree No. 72/2013/ND-CP on management, provision and use of Internet services and online information.
Gambling Act, Bulgaria (2012), http://www.dkh.minfin.bg/document/403.
Law on Consumer Protection (No. 59/2010/QH12) and Decree No. 52/2013/ND-CP on e-commerce.
Law on E-Transactions (No. 51/2005/QH11).
Law on Information Technology (No. 67/2006/QH11); Law on Network Information Security (No. 86/2015/QH13).
Ministry of Communications & Informatics Regulation No. 20 of 2016 regarding the protection of personal data in an electronic system (the MOCI Regulation).
Personal Information Protection Act (promulgated by the Ministry of Justice, Taiwan, May 26, 2010), <http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021>.
Personally Controlled Electronic Health Records Act 2012, no. 63, Australia (2012)
Regulation of the Government of the Republic of Indonesia No. 82 of 2012 concerning Electronic Systems and Transaction Operation (Reg. 82).
Regulation on the Credit Reporting Industry, State Council 228th session, China (2013), <http://www.pbccrc.org.cn/crc/jgyhfw/201309/1ca0f775b50744cabaf83538288d77a9/files/e8a8bf080ed6 4f48914a652da1d8fdc3.pdf.>
The Civil Code of Vietnam (No. 91/2015/QH13).
The Malaysia's Personal Data Protection Act 2010 (PDPA).
The Philippines' Data Privacy Act of 2012 (Republic Act No. 10173).
The Singapore's Personal Data Protection Act 2012 (No. 26 of 2012).