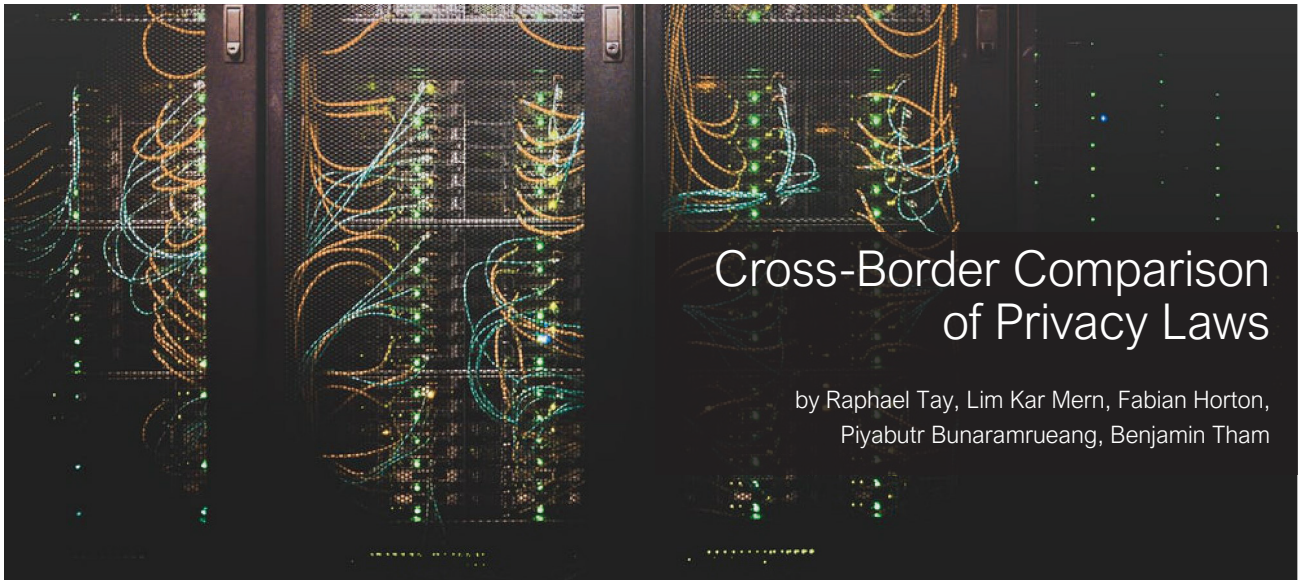

Cross-Border Comparison of Privacy Laws

by Raphael Tay, Lim Kar Mern, Fabian Horton, Piyabutr Bunaramrueang, Benjamin Tham

Since Facebook's massive data privacy breach exposé in early 2018, internet users have been extremely cautious about sharing their personal data online, be it through a social networking platform, job application or the use of a product application. Coupled with the increasing media awareness of privacy rights is Europe's General Data Protection Regulation (GDPR), which was implemented in May 2018 and has had a ripple effect throughout the global economy.

With the proliferation of innovative products and services and the increase in cross-border merger and acquisition (M&A) activity in ASEAN and Oceania, the importance of data security has been a great concern to individuals and is at the forefront of every business's best practices, especially of multinational corporations. From processing personal data of employees or suppliers in a deal, to disclosure of documents in a data room, data protection (or the lack thereof) poses substantial risks and may critically affect the success of M&A transactions.

We shall compare how some countries — namely, Thailand, Malaysia, Australia and Singapore — are performing in ensuring adequate standards of data protection and whether we should also be adopting a regional approach in the protection of personal data.

Raphael and Kar Mern, along with the following co-authors from Australia, Thailand and Singapore, provide their views on personal data protection laws from the perspective of their own jurisdiction in this article.

FABIAN HORTON is a lecturer at the College of Law (Australia) and the principal solicitor at ConnectLaw in Victoria, Horton is a solicitor with substantial experience in the field of technology and law and has published extensively in the area, including being the lead author of the Law Council of Australia cybersecurity initiative "Cyber Precedent". He is the founding chairperson of the Technology and the Law Committee of the Law Institute of Victoria.

PIYABUTR BUNARAMRUEANG is a lecturer at the Faculty of Law in Chulalongkorn University, Thailand. His area of specialisation is in communications law and policy, personal data protection and cybersecurity. In addition to contributing to the literature on law and policy reform of the telecommunications industry in Thailand, Piyabutr has also written extensively on the telecommunications business in US and EU; and the topic of intellectual property in the age of information and the internet.

BENJAMIN THAM holds Bachelors' degrees in science and law from the National University of Singapore and the University of Nottingham, respectively, and is admitted to the Singapore Bar. Tham is currently a research associate at the Centre for AI and Data Governance and an adjunct lecturer at the School of Law, Singapore Management University. His research areas are primarily in intellectual property and technology law. He is also a legal associate at David Llewelyn & Co LLC and an assistant editor of the Singapore Arbitration Journal.

By way of background, the following definitions have been extracted from the GDPR, and unless expressed otherwise, "*processing*" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure of destruction; "*data user"* means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; "*data processor*" means a natural or legal person, public authority, agency or other body which process personal data on behalf of the data user; and "*data subject*" means an individual who is the subject of the personal data.

(1) What are the circumstances in which consent to process personal data from the data subject is not required?

Catchwords: *Prevention of crime – anonymised research – necessity – performance of a contract – legal obligation to comply with law*

MALAYSIA:[1] Some of the exemptions are prevention of crime and carrying out anonymised research and if the processing is necessary for, among others, the performance of a contract that the data subject is a party to or if the data user has a legal obligation to comply with any law.[2]

Catchwords: *Necessity – Second, Third and Fourth Schedules – collection, use and disclosure, – emergency – life, health or safety – artistic or literary purposes – data publicly available*

SINGAPORE:[3] Exceptions lie in s 17 of the PDPA, which expressly provides that an organisation may collect, use and disclose personal data about an individual, without consent or from a source other than the individual, only in the circumstances and subject

1 The processing of personal data is premised on seven data protection principles ("PDPA Principles") under the Personal Data Protection Act 2010 [Act 709] ("PDPA"), one of which provides for the requirement of consent from the data subject ("General Principle"). Consent may be expressed or implied from conduct as long as the data subject has been informed of the purpose and proposed processing of their personal data.

2 Section 6(2) of Malaysia's PDPA provides that the exception to consent includes:
- (a) the performance of a contract that the Data Subject is a party to;
- (b) taking the steps at the request of the Data Subject with a view to entering into contract;
- (c) compliance with any legal obligation to which is the Data User is subject (other than by contract);
- (d) protecting the vital interests of the data subject;
- (e) the administration of justice; or
- (f) the exercise of any functions conferred on any person by or under any law.

3 The general position under the Singapore Personal Data Protection Act 2012 ("PDPA") in relation to consent is provided under s 13 of the PDPA, which prohibits organisations from collecting, using or disclosing personal data about an individual unless "the individual gives, or is deemed to have given, his consent" pursuant to the PDPA in relation to the collection, use or disclosure as the case may be.

to any condition in the Second, Third and Fourth Schedules of the PDPA, respectively, for example where is it necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual, for artistic or literary purposes, or where the personal data is publicly available.

Catchwords: *Australian Privacy Principles – consent as exception to general prohibition – consent for authority to handle in a particular way – required for authority's function or activity*

AUSTRALIA:[4] In some of the Australian Privacy Principles (APP), consent is an exception to a general prohibition against personal information being handled in a particular way. In others, consent provides authority to handle personal information in a particular way. In general, organisations cannot collect any information that they like, they may only collect information that they require for their function or activity (APP 6).[5]

Catchwords: *Vital interest – incapable of consent – contractual obligation – public reasons by official authorities – legitimate interests – legal obligations*

THAILAND:[6] The five lawful bases in which consent is not required from the data subject are:

(a) to protect the vital interest of the data subject, where the data subject is incapable of giving consent;
(b) where there is a contractual obligation (or where there is intention to enter into contract);
(c) public task carried out by official authorities or in the exercise of official authority vested in the data user;
(d) where there is legitimate interest of a data user or a third party; and
(e) legal obligations of data user.

(2) Can the law hold data processors liable for a breach of personal data if they are based outside of the country?

Catchwords: *Data processor not directly accountable under PDPA – data processing agreement – obligations on data processor – technical and organisational security measures – contractual liability*

MALAYSIA:[7] Unlike the GDPR, the PDPA does not expressly provide for data processors to be directly accountable for any data breach. In fact, the provisions of the PDPA are drafted with the intention to hold the data user responsible for complying with the PDPA principles. For example, if the data user is a large corporation engaging in the services of a

4 The processing of personal data is governed primarily by the Privacy Act 1988 ("Privacy Act"). The Privacy Act includes 13 Australian Privacy Principles (APPs) that regulate the handling of personal information by certain companies and Australian government agencies (APP entities). The Australian Privacy Principles guidelines note that "[c]onsent is relevant to the operation of a number of APPs.

5 For clarity, the term "processor" is not used in the Privacy Act but the APPs apply to APP entities to the extent that they hold personal information and according to the Office of the Australian Information Commissioner ("OIAC"), this is sufficient to cover outsourced service providers, i.e. "processors". APP entities are therefore either data users and/or data processors for the purpose of this article.

6 Except for a few provisions in the Thailand Personal Data Protection Act ("PDPA"), the law has been in effect since 28 May 2019 and was modelled very closely after the GDPR.

7 The data processing agreement imposes obligations on the data processor to meet the standards of protection higher or equivalent to those of the PDPA and at the same time provide that the data user be indemnified if the data processor causes a data breach. The liability of the data processors is therefore a contractual one. As for the data user, he may be liable to a fine not exceeding RM300,000 (approx. USD75,000).

data processor located outside of Malaysia, then it becomes imperative for the data user to enter into a form of data processing agreement to ensure that that the data processor provides sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out.

Catchwords: *Data processor not expressly defined in PDPA – definition of "organisation" includes the role of a data processor*

SINGAPORE: It should be firstly noted that the PDPA does not make reference to data processors (unlike the GDPR). The PDPA does not contain a specific provision for extraterritorial operation. A "data processor" based outside of Singapore, however, may still be liable under the PDPA if it qualifies as an "organisation" which fails to comply with any of the PDPA provisions in relation to data breaches as a data user,[8] for example, an organisation's obligation to protect personal data by making reasonable security arrangements.[9]

Catchwords: *Data user responsible for breach – breaches of APP – mandatory data breach notification*

AUSTRALIA: The Privacy Act provides for the data user to be responsible for any breach of personal data.[10] For example, it is the data user who must comply with the Notifiable Data Breach law even if the information breach occurred with respect to a data processor who was not located in Australia.[11]

Catchwords: *Extraterritorial applicability – similar to GDPR – liable if data processor based in Thailand – regardless of location – data subjects in Thailand – monitoring of data subjects in Thailand*

THAILAND:[12] Similar to the extraterritorial applicability of the GDPR, the data processor will be held liable under Thailand's PDPA if:

(a) they are based in Thailand, regardless of whether the processing takes place in Thailand;
(b) the processing of data subjects in Thailand, by a data processor not in Thailand; and
(c) the monitoring of data subject's behaviour which takes place in Thailand.

(3) What are the circumstances in which personal data obtained in your jurisdiction may be transferred to third countries?

Catchwords: *Transfer of personal data – s 129(3) PDPA exceptions – White List of countries not yet gazetted*

8 This is because s 2(1) of the PDPA defines an "organisation" widely as including any individual, company, association or body of persons, corporate or unincorporated, regardless of whether they are formed or recognised under Singapore law and regardless of whether they are resident or have a place of business in Singapore.

9 PDPA, s 24. The general penalty for a breach under s 24 is a fine not exceeding SGD10,000 (USD7,268).

10 Data breach laws operate in Australia under the ss 26WA-26WT of the Privacy Act. These sections make it mandatory for APP entities, in this case data users, to make certain notifications of any eligible data breach. Such a breach is "when personal information held by an agency or organisation is lost or subjected to unauthorised access, use, modification, disclosure or other misuse". And that the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

11 The Notifiable Data Breach laws contains a list of requirements that must be followed in the event of an eligible data breach. Failure to comply with the requirements of Notifiable Data Breach laws can result in fines of up to AUD360,000 (approx. USD247,000) for individuals and approximately AUD1.8 million (approx. USD1.23 million) for companies.

12 Data processors can now be held accountable under the PDPA, where such accountability was only previously limited to contractual liability of the data processing agreements between the data user and data processor. The penalties of any breach in this case are punishable by fines up to THB5 million (approx. USD164,000) or imprisonment up to one year and/or fines up to THB1 million (approx. USD32,819)

MALAYSIA: [13] Personal data may only be transferred out of Malaysia if they fall under any of the circumstances listed in s 129(3) of the PDPA, such as when the data subject has given his consent to such transfer, or if the data user has taken all reasonable precautions and exercised all due diligence to ensure that personal data will not be processed in contravention with the provisions of the PDPA.[14]

Catchwords: *Limitations on transfer outside of Singapore – s 26 PDPA – appropriate steps to safeguard data – third party to have protection standards comparable to PDPA*

SINGAPORE: Section 26 of the PDPA provides for limitations to the transfer of personal data by a data user outside of Singapore.[15] The data user must ensure that appropriate steps are in place to safeguard data protection; and that the recipient of the third country is bound to a standard of protection that is comparable to those stated under the PDPA. It should be noted that the section, however, does not govern business contact information or data intermediaries (i.e. data processors).[16]

Catchwords: *Reasonable steps to ensure APPs are complied with – unless otherwise exempted in APP 8 – necessity by law – consent by data subject for cross-border transfer*

AUSTRALIA:[17] Before an APP entity or data user discloses or transfers personal data outside of Australia, they must take "reasonable steps" to ensure all of the APPs are not broken, unless the disclosure meets any of the exceptions outlined in APP 8, such as when the disclosure of information is required by Australian law or if the data subject consents to the cross-border transfer of his personal data to a foreign entity.

Catchwords: *Adequate level of protection – prescribed by Personal Data Protection Commission – unless otherwise necessary for public interest – explicit consent to the transfer by data subject*

THAILAND: Data users can only transfer personal data to foreign countries or international organisations with adequate level of protection, as prescribed by the Personal Data Protection Commission ("PDPC"). In the absence of this, personal data may only be transferred to a country outside of Thailand if they meet any of the derogatory conditions as prescribed under the law similar to Art 49 of the GDPR, which includes circumstances where the transfer is necessary for public interest or when the data subject has explicitly consented to the transfer.

(4) If a data user in your jurisdiction suffers a security incident resulting in a breach of confidentiality, availability and integrity of personal data, what are the steps required by law that he must take as a data user to address the breach?

Catchwords: *No statutory obligation to report data breaches – complaint of alleged breach to the*

13 A "White List" proposed in a Public Consultation Paper (No 1/2017) was published by Malaysia's Personal Data Protection Commissioner ("Commissioner") containing a list of countries that had comprehensive data protection legislation to permit the transfer of personal data to third countries without fulfilling s 129(3). Some of those countries are Australia, Singapore, China, the Philippines and those in the European Economic Area. However, the White List has not yet been issued as an order and, as such, does not have any force of law.

14 For example, if acquiring consent is not practicable, the data user may transfer data if he ensures that a data processing agreement with the data processor (outside of Malaysia) contains data protection provisions that are of higher or equivalent standards as those contained in the PDPA. 15 Section 26(1) of Singapore's PDPA provides for the general position that "[a]n organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under [the PDPA] to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under [the PDPA]."

16 The requirements for transfer of personal data outside of Singapore can be found in the Personal Data Protection Regulations 2014 ("the PDPR"). In particular, regulation 9 provides for the requirements for transfer, which include, but are not limited to, taking appropriate steps to ensure that the transferring data user will comply with Parts III to VI of the PDPA (which govern the various obligations, such as access and correction) and also to ascertain whether, and to ensure that, the recipient of the personal data in that country outside Singapore is bound by "legally enforceable obligations" to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA. What constitutes as "legally enforceable obligations" is provided for under regulation 10.

17 Under the Australian Privacy Act, the APP entities or data user must comply with the legislation regardless of where the data is held.

Commissioner – reasonable grounds – investigation – issuance of enforcement notice – remedy of such breach

MALAYSIA: Unlike the GDPR and guidelines imposed by Bank Negara Malaysia on certain financial services providers in Malaysia,[18] there are currently no statutory obligations to report or notify data breach incidents to the data subjects and/or the PDPA Commissioner ("Commissioner") under the PDPA.

However, an official complaint of the alleged breach may be made by any person under the PDPA and if the Commissioner has reasonable grounds to believe that it contravenes the provisions of the PDPA, then upon investigation by the Commissioner, an enforcement notice may be issued on the data user specifying and directing, among others, the steps and period by which to remedy such breach.[19]

***Catchwords**: No mandatory notification – unless a critical information infrastructure under Cybersecurity Act – non-binding guidelines – recommendations to notify affected individuals*

SINGAPORE: If a data user qualifies as a critical information infrastructure ("CII") under the Singapore Cybersecurity Act ("CA"), s 14(1) CA would apply.[20]

For other data users other than those described above, however, there is no mandatory notification obligation for organisations to inform the Singapore Personal Data Protection Commission ("PDPC") of security incidents. The PDPC has non-binding guidelines which recommend data users to, *inter alia*, notify affected individuals and the PDPC in the event of a data breach incident.[21]

***Catchwords**: Notifiable Data Breach – APP entity or data user to make assessment of breach – remedial action – notify the Australian Information Commissioner – reporting requirements to relevant authorities*

AUSTRALIA: Notifiable Data Breach laws under the Privacy Act stipulate that if an eligible data breach is suspected, the APP entity must make an assessment of the breach and attempt to take remedial action in relation to the breach. The APP entity must also notify individuals whose personal information is involved and notify the Australian Information Commissioner. In addition to the Privacy Act, depending on the type of data breach, certain APP entities may have reporting requirements to the Australian Taxation Office, Australian Securities and Investments Commission, and the Australian Cyber Security Centre.

***Catchwords**: Data user obligation – 72 hours' notice to Committee – unless risk to data subject is unlikely – measures to mitigate if risk is high*

THAILAND: If a data breach takes place, the data user will have an obligation, within 72 hours of notice, to inform the Personal Data Protection Committee without undue delay, unless the breach is unlikely to result in a risk to the data subject. If the breach is likely to result in a high risk to data subjects, the data user must take subsequent measures to mitigate the risk to the data subjects.

18 Bank Negara Malaysia ("BNM") had, on 17 October 2017, issued a guideline entitled "Management of Customer Information and Permitted Disclosures", setting out that financial service providers must notify BNM and law enforcement agencies if any data breach brings any harm or threat to the public. Unlike the GDPR, customers (or data subjects in the context of the PDPA) will only be notified by way of a public announcement if the breach affects a large number of customers.

19 Any failure to comply with the notice is a criminal offence and would be liable to a fine not exceeding RM200,000 (approx. USD50,000) or to imprisonment not exceeding two years, or both.

20 Section 14(1) CA provides that the owner of the CII must notify the Commissioner of Cybersecurity of the occurrence of a prescribed cybersecurity incident in respect of the CII. Such prescribed cybersecurity incident in respect of any computer or computer system under the owner's control that is interconnected with or that communicates with the CII, or any other type of cybersecurity incident in respect of the CII that the Commissioner of Cybersecurity has specified by written direction to the owner, must be notified within the prescribed period in the prescribed form and manner after becoming aware of such occurrence.

21 The PDPC has announced plans to introduce a mandatory breach notification regime as part of the proposed amendments to the PDPA.

(5) How are CCTV images dealt with as personal data under the privacy laws of your jurisdiction?

Catchwords: *CCTV images – commercial purposes – personal data under PDPA – Proposal Paper No 5/2014 – Guideline on how to use CCTV images in accordance with PDPA Principles – no developments since Proposal Paper – not yet gazetted*

MALAYSIA: CCTV images that identify a person fall under the definition of personal data in the PDPA. Any CCTV images used for commercial purposes would therefore be subject to the PDPA in Malaysia.

A Proposal Paper (No 5/2014) entitled "Guide on the Management of CCTV under PDPA 2010" was issued by the Commissioner's department in 2014 to provide a guideline on how to use CCTV images in accordance with the PDPA principles. For example, at a workplace, the General Principle prescribes that consent is not required for processing of CCTV images if the purpose of processing is for the prevention of crime; and in accordance with the Disclosure Principle, the data user (employer) must only disclose such CCTV images of the data subject (employees) to assist in the prevention of crime and not for any other purposes. However, since the publication, there have not been any further developments on the Proposal Paper.

Catchwords: *CCTV images – personal data under PDPA – obligations on data user – where consent is not required, no obligation to provide notification unless for managing or terminating employment relationship*

SINGAPORE: CCTV images are considered as personal data under the PDPA and the obligations in the law apply to data users of CCTV images.[22]

Where consent is not required, for example, where the circumstance falls under the Second, Third or Fourth Schedules of the PDPA (which provide for the collection, use or disclosure of personal data without consent, respectively), there is no obligation imposed by the PDPA on the data user to provide notification (see s 20(3) of the PDPA) unless it is in relation to the collection, use or disclosure of personal data about an individual for the purpose of managing or terminating an employment relationship between the data user and that individual (see s 20(4) of the PDPA).

Catchwords: *CCTV images – any surveillance device – compliance with the APPs*

AUSTRALIA: CCTV images are recognised as personal data under the Privacy Act and any personal information collected through a surveillance device must comply with the APPs.

Catchwords: *CCTV images – processed to offer goods or services – monitor behaviour of people in Thailand – including deployment of any advanced technologies – facial recognition*

THAILAND: If the CCTV images are being processed to either offer goods or services; or monitor the behaviour of the people in Thailand, then these would be regulated by the PDPA.

As CCTV images fall within the meaning of personal data, the PDPA applies to the collection of them, including the deployment of any further advanced technologies such as

22 The consent obligation and notification obligation under the PDPA requires data users to inform individuals of the purposes for which their personal data will be collected, used or disclosed in order to obtain their consent (see ss 14 and 20 of the PDPA in general). Notifications should, therefore, be provided by data users in order to fulfil the two aforesaid obligations to obtain consent for the collection, use or disclosure of CCTV images.

facial recognition. The PDPA requires a risk assessment and security measures to mitigate such risks in the same way DPIA (Data Protection Impact Assessment) is required by the GDPR.

Our Views

With the exception of certain legislative idiosyncrasies,[23] the principles of personal data protection in these four countries seem to be falling in line with the current of GDPR in tow as a global standard for data protection.

The Asia Pacific Economic Cooperation (APEC) developed the Cross-Border Privacy Rules (CBPR) System,[24] and similar to the GDPR, it was established by APEC with the view of assisting the members in achieving a common regional approach in data protection; and although only a handful of countries have signed up for the voluntary scheme — the US, Mexico, Japan, Canada, South Korea and Singapore — the region that the CBPR covers is too expansive and fragmented because of the disparity in history, cultural and socio-political directions. Furthermore, with Thailand having protection standards and extraterritorial powers equivalent to that of the GDPR, the CBPR may not have any long-term effect on any data regulation in the region.

Perhaps the answer to better protection of personal data lies not in whether there should also be a regional approach, rather entities in control of personal data should be compelled to make their data security systems and mechanisms more transparent and readily accessible by the data subjects in terms of understanding the entity's protocols or having a person in charge to readily communicate on data processing.

Rather than waiting for enforcement agencies to come down like a sledgehammer, perhaps empowering data subjects to take more control over their personal data is a first step forward in ensuring better data protection such as allowing data subjects opt in rather than opt out of letting their personal data being used or giving data subjects more flexibility about when and where their personal data may be used. As once said by Jen King, director of consumer privacy at the Center for Internet and Society, Stanford Law School, "People may want some of the convenience of these things, but that doesn't mean they want them in every facet of their life." **LH-AG**

23 For example, Thailand being the only country to have extraterritorial effect; Malaysia and Australia holding the data user (and not the data processor) ultimately responsible for personal data breaches.

24 Asia Pacific Economic Cooperation, Cross-border Privacy Rules (2005) <https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System> (accessed 30 September 2019).