ASIAN BUSINESS LAW INSTITUTE

Comparative Table of Laws and Regulations on Cross-Border Personal Data Flows in Asia

(Working Document, May 28, 2020)

PRESENTATION

This document consists in a comparative Table on the Laws and Regulations relative to cross-border transfers of personal data in fourteen Asian jurisdictions.

This Table was originally drafted to support the write-up by ABLI of a comparative review of those laws and regulations (also available at https://abli.asia), with the following objectives:

- revealing the different causes of legal fragmentation between such provisions in the region;
- identifying the collective benefits of legal convergence and certainty in this area of the law for organisations to which multiple legal frameworks apply, individuals whose personal data is transferred across borders, and privacy regulators in the context of ensuring regulatory cooperation and consistent regulatory action; and
- setting out proposals for how Asian public stakeholders may promote legal certainty and greater consistency between their respective data transfer regimes in the region.

A recurring difficulty for stakeholders in Asia is simply gaining access to laws, regulations, and regulatory guidance on data privacy and data transfers in the region. ABLI has therefore decided to publish this Table, which it has drawn up to inform its analysis, for the benefit of all.

The table is current as at **28 May 2020** and will be regularly updated on ABLI's website.

METHODOLOGY

Jurisdictions covered

The jurisdictions assessed in this Review are those covered in ABLI's Data Privacy Project: Australia, China, Hong Kong SAR, India, Indonesia, Japan, Macau SAR, Malaysia, New Zealand, Philippines, Singapore, South Korea, Thailand, and Vietnam

See ***https://abli.asia/projects/data-privacy-project***

Legal grounds, mechanisms, schemes considered

The legal grounds, mechanisms, and schemes for transfers considered in this Review are:

- *Firstly*, those most commonly found in data protection regimes globally, including recently promulgated Data Protection Laws that have taken inspiration from EU GDPR; and
- *Secondly*, those considered for inclusion in Asian regional frameworks— including the ASEAN Digital Data Governance Framework.

Specific instruments that do not fall into these categories have therefore not been considered (e.g. international agreements).

Exclusion of sectoral laws

Sector-specific requirements (e.g. in telecom, banking, credit reporting, or health sectors) have not been reviewed in this Review so as to avoid too wide a field of comparison.

Data localisation and data transfer mechanisms

In this table we include sweeping localisation obligations that apply cross-sector to online activities (e.g. 'network providers') in four legal systems (China, India, Indonesia, and Vietnam).

Sectoral or targeted localisation requirements (e.g., electronic health records; tax information; or personal credit information) are not considered here, except in those four jurisdictions where they articulate with broader localisation requirements and the data protection law (in force or in draft).

Legislative proposals considered

Given the substantial legislative activity currently taking place in the area of personal data protection and privacy in Asia, this Review includes legislative proposals that should soon be passed into law in select key jurisdictions (India, Indonesia, New Zealand).

TABLE KEYS

Consent

For each jurisdiction, the applicability of consent under the Data Protection Law or Bill is expressed as:

- YES (required) or YES (optional), where the individual's consent is a systematic requirement that may be waived only exceptionally or is one among several legal bases for transfers;
- NO, where obtaining the individual's consent is irrelevant in the structure of the applicable legal regime.

Adequacy, white lists; Self-assessment of the level of protection in the country of destination; Contractual safeguards; Binding Corporate Rules; Certification; Codes of conduct

For each jurisdiction, the applicability of such mechanisms or schemes for data transfers under the Data Protection Law or Bill is expressed as:

- YES where the legal regime explicitly confirms their applicability;
- NO where the legal regime is silent on their applicability;
- UNCERTAIN where the legal regime fails to address the point straightforwardly; and
- CONCEIVABLE where clarification could be provided in implementing regulations or guidance, but the regulator (when there is one) has not provided such clarification.

APEC Cross Border Privacy Rules (CBPRs)

In this Section, jurisdictions are marked as:

- YES, if they have joined the system as CBPR member countries and either have an existing legislative framework in place to recognise the CBPR; or have recognised CBPR as a transfer mechanism, where applicable restrictions exist; and
- NO, if they are not a member of APEC economy and thus cannot join the CBPR system; or in respect of those jurisdictions that are members of APEC, they have expressed no interest in joining the system, and hence a unilateral recognition of CBPR as a sufficient mechanism for transfer is remote or unlikely.

Exemptions, additional legal grounds

In this section we consider the specific circumstances defined by statute under which data may flow from Asian jurisdictions, irrespective of the implementation of data transfer mechanisms or schemes, the level of protection in the country of destination, or obtaining the data subject's consent.

For each jurisdiction, the admission that personal data transfers may take place in such situations is expressed as:

- STATUTORY EXEMPTION, where the law lists a series of circumstances in which it appears necessary to derogate to the main data transfer rules in the Data Protection Law or Bill (e.g., consent, adequacy);
- EXEMPTION BY THE AUTHORITY, OR BY THE GOVERNMENT, where the law leaves a certain latitude to the public authorities to authorise organisations to derogate from the data transfer rules in specific circumstances; or
- ADDITIONAL LEGAL GROUND, where such situations are recognised in the law but operate autonomously with the main data transfer rules, instead of in the form of exemptions or derogations.

Where no exemption from the default position applies, the applicable data transfer regime is marked as NO.

TABLE OF CONTENTS

Jurisdictions Relevant Laws and Regulations Main Principle and Exceptions	Consent	White Lists, Adequacy Findings	Self-Assessment by Organisation of Overseas Level of Protection	Contractual Safeguards	Binding Corporate Rules (BCRs)	Certification	APEC Cross Border Privacy Rules (CBPRs)	Codes of Conduct	Exemptions & Additional Legal Grounds for Transfers
AUSTRALIA **Privacy Act (1988)** **Australian Privacy Principle 8.1 (APP 8.1)** *Accountability Principle*. Before an entity discloses personal information to an overseas recipient, the entity must *'take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to that information.'* **S16C:** If an entity discloses personal information about an individual to an overseas recipient and APP 8.1 applies to the disclosure of the information, the entity is accountable for any acts or practices of the overseas recipient that would breach the APPs in relation to the information. Chapter 8 of the Australian Privacy Principles Guidelines (**APP Guidelines**) (Cross-border disclosure of personal information) published by the Office of the Australian Privacy Information Commissioner (OAIC) outlines how the OAIC will interpret APP 8. *Note regarding 'use' and 'disclosure' of personal information:* The focus of APP 8 is on the 'disclosure' of personal information to overseas recipients, as opposed to the 'use' of the information. While neither 'use' or 'disclosure' is defined in the Privacy Act, an entity *'discloses personal information when it makes it accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control'* (APP Guidelines, para B.64).	**YES (optional)** The accountability principle in APP 8.1 does not apply where the individual consents to the cross-border disclosure after the entity informs the individual that APP 8.1 will no longer apply (APP Guidelines at para. 8.27 ff.). Consent means 'express consent or implied consent' (Privacy Act s 6(1)). The four key elements of consent are (APP Guidelines, Chapter B 'Key Concepts', Para. B.35): - the individual is adequately informed before giving consent; - the individual gives consent voluntarily; - the consent is current and specific; and - the individual has the capacity to understand and communicate their consent. Each of these key elements are explained in detail in the APP Guidelines (B.36-58).	**NO** The OAIC does not endorse 'white lists' so a subjective assessment is required under APP 8.1.	**YES** APP 8.1 does not apply where the entity reasonably believes that the recipient is subject to '*a law, or binding scheme*' *that is overall 'substantially similar to the way in which the APPs protect the information*', and there are mechanisms available to the individual to enforce that protection (APP 8.2(a)).	**YES** To discharge APP 8.1 it is generally expected that an APP entity will enter into an enforceable contractual arrangement with the overseas recipient that requires the recipient to handle personal information in accordance with the APPs (APP Guidelines para. 8.16). Where an Australian government agency discloses personal information to a recipient that is engaged as a contracted service provider, the agency must take contractual measures to ensure that a contracted service provider does not do an act, or engage in a practice that would breach an APP if done by that agency (S95B). The contract must contain provisions to ensure that such an act or practice is not authorized by a subcontract (S95B(3). Contractual measures under section 95B will generally satisfy the requirement in APP 8.1. (APP Guidelines, para 8.18).	**YES** APP 8.1 does not apply where the entity reasonably believes that the recipient is subject to a *'binding scheme that is overall substantially similar to the APPs'*, and there are mechanisms available to the individual to enforce that protection (APP 8.2(a)). An overseas recipient may be subject to a binding scheme where, for example, it is '*subject to Binding Corporate Rules (BCRs)*' (APP Guidelines, para 8.21)	**CONCEIVABLE** APP 8.1 does not apply where the entity reasonably believes that the recipient is subject to a *'binding scheme that is overall substantially similar to the APPs'*, and there are mechanisms available to the individual to enforce that protection (APP 8.2(a)). An overseas recipient may be subject to a binding scheme where, for example, it is *'subject to an industry scheme'* that is enforceable once entered into, irrespective of whether the recipient was obliged or volunteered to participate or subscribe to the scheme (APP Guidelines, para 8.21)	**YES** Australia was endorsed as a participating economy in the CBPR system on November 23, 2018. The CBPR system has not yet been implemented in Australia, and no Accountability Agent has been appointed to operate in Australia. The OAIC will be responsible for regulating the CBPR system in Australia, once implemented.	**CONCEIVABLE** *(provided the code is effectively binding on the overseas organisation)* While APP 8.1 does not apply where the entity reasonably believes that the recipient is subject to a *'binding scheme that is overall substantially similar to the APPs'*, and *'there are mechanisms available to the individual to enforce that protection*' (APP 8.2(a)), the Privacy Act does not mention the possibility for an organisation to discharge the requirements of APP 8.1 by providing safeguards through a non-binding code of conduct or practice. An overseas recipient may be subject to a binding scheme where, for example, it is *'subject to a privacy code'* that is enforceable once entered into, irrespective of whether the recipient was obliged or volunteered to participate or subscribe to the scheme (APP Guidelines, para 8.21). However, such a code does not replace APPs, but operates in addition to the requirements of the APPs. An overseas recipient may not be subject to a law or binding scheme where the recipient can opt out of the binding scheme without notice and without returning or destroying the personal information (APP Guidelines at para 8.22).	**DEROGATIONS TO APP 8.1** APP 8.1 does not apply to the transfer of personal information to an overseas recipient where (APP 8.2): - the disclosure is *'required or authorised by or under an Australian law or a court/tribunal order'*; - the disclosure is required or authorised under an '*international agreement relating to information sharing to which Australia is a party'*; - the disclosure is necessary for an enforcement related activity; - a *'permitted general situation'* exists in relation to the disclosure of the information by the entity, i.e. the disclosure is necessary to: 1. lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety (S16A(1), Item 1); 2. in relation to suspected unlawful activity or serious misconduct; 3. locate a person reported as missing; 4. for a diplomatic or consular function or activity; 5. for certain Defence Force activities outside Australia.
CHINA **Cybersecurity Law (CSL) 6 November 2016** *(effective June 2017).* **Art 37:** '*Critical Information Infrastructure Operators'* (CIIOs) must store personal information and *'important data'* collected and generated in China and may transfer such information and data overseas only for business needs and upon security assessment by the relevant authorities. Where due to business	**YES (required)** In principle informed consent of the individual is necessary for all *'network operators'* to transfer or disclose any persona data to a third party (inside or outside China) (CSL, Art 42). Consent may be obtained through 'proactive' (i.e. voluntary) personal actions but may occasionally be implied from the data subject's actions (Guidelines for Cross-Border Data Transfer Security of the National Information Security Standardisation Technical Committee (TC260), August 2017).	**NO** The CAC is due to issue implementing regulations for the transfer requirements in Art 37 CSL. The latest draft measures released by CAC (dated 13 June 2019) are applicable to all 'Network Operators' (not only CIIOs) and 'personal information'. They require that all network operators must apply for a security assessment of the contemplated transfers to the provincial branch of the CAC for review (i.e. no differentiation is made depending	**NO** The prior draft Measures (April 2017, revised in May and August 2017) provided for a self-assessment of the contemplated transfers and that the authorities would make such assessments only in specific cases. The last draft of June 13, 2019 comes back on this position and requires that all network operators must apply for a security assessment of the contemplated transfers to the provincial branch of the CAC for review (i.e. no differentiation depending on	**YES (required)** The draft Cross-Border Transfer Assessment measures provide that the elements to be notified to the provincial CAC for assessing the security of the transfer must provide, among others, *'the contract entered into between the network operator and the recipient'* (Art 4). The contract will be part of the elements assessed by CAC, with a focus on whether the terms of the contract can fully safeguard the legitimate rights and interests of the data subject.	**UNCERTAIN** The draft Cross-Border Transfer Assessment measures provide that the elements to be notified to the provincial CAC for assessing the security of the transfer must provide, among others, *'the contract entered into between the network operator and the recipient'* (Art 4). In contrast, Art 13 of the draft measures refer to *'the contracts or other legally binding measures ('the Contracts')'*. It is possible that Internal Rules, if they are effectively *'binding'* under	**NO** The draft Cross-Border Transfer Assessment measures do not include overseas certification schemes in the relevant assessment factors. An information security certification scheme run by the Information Security Certification Centre of China is operating but is not a strict equivalent of existing 'data protection trust marks' or 'privacy seals' in the region.	**NO** China is an APEC Member Economy but has not indicated an intention to join CPEA or CBPRs.	**NO** The draft Cross-Border Transfer Assessment Measures do not consider adherence to a code of conduct as a relevant factor in the security assessment to be carried out by CAC or its local branches.	**NO** Art 9.5 of the Personal Information Security Specification GB/T 35273/2020 provides for exemptions from the default requirement to obtain consent from personal information subjects to 'transfer their data' (e.g. for fulfilment of obligations under laws and regulations by the controller; national security and national defense; public safety, public health, and significant public interests; criminal investigation, prosecution, trial, and judgment enforcement, etc.) <u>but</u> this

requirements it is *'truly necessary'* to provide personal information outside PRC, CIIOs shall follow the measures of State Network Information Dept and State Depts (unless laws or regulations provide otherwise) to conduct a cross-border transfer security assessment. Note: Sectoral localisation obligations prevail over Art37 CSL, e.g. in banking, insurance, credit reporting, health and genetics, online taxi booking and location apps. Art37 CSL to be combined with: **Personal Information Security Specification issued by the National Information Security Standardisation Technical Committee (TC260) (GB/T 35273/2020), Art 9(8)** *(entry into force October 1, 2020)* With regard to the cross-border transfer of Personal information collected and generated in China, the personal information controller *'shall comply with the requirements of relevant national regulations and standards*'. **Draft Cross-Border Transfer Assessment measures of the Cyberspace Administration of China (CAC)** (*pending- draft version June 13, 2019)* The draft measures expand the scope of the transfer measures in Art37 CSL to all *'Network Operators'* (not only CIIOs) and *'personal information'*. Network operators are *'owners and administrators of networks and network service providers'* (Art 76 CSL). Network Operators must apply for a security assessment of the contemplated transfers to the provincial branch of the CAC for review (i.e. no differentiation depending on sensitivity levels). *Note:* Sectoral localisation obligations prevail over Art 37 CSL, e.g. in banking, insurance, credit reporting, health and genetics, online taxi booking and location apps.	Limited exceptions to consent for international transfers may apply (see next), but security assessment requirements will in any case remain applicable.	on sensitivity levels). It does not appear that the security assessment will explicitly include an assessment of the level of personal data protection in third countries (contrary to what was contemplated in a previous draft).	sensitivity levels).	The draft sets out the terms and conditions required to be in contracts between data transferors and offshore data recipients (Arts 13 and 16). The detailed obligations are broadly similar to the EU SCCs, with differences relating to compensation to data subjects and onward transfers. The contract must state the purpose of the transfer, the types of information provided and their storage period. Data subjects should be beneficiaries under the contract but could also obtain compensation in case of breach by any of the parties or both (unless the parties can prove that they are not liable, thus reverting the burden of proof). They have the right to be informed and to request copies of such a contract.	PRC law and contain the required elements in the draft measures, would be considered adequate for the purpose of the security assessment by CAC.				provision is only in relation to domestic transfers. The current version of the Draft Cross-Border Transfer Assessment measures does not clearly provide for like exemptions from consent or contract.
HONG KONG SAR **Personal Data (Privacy) Ordinance (Cap. 486), s 33** [*not yet in force).* Transfers of personal data to overseas jurisdictions are forbidden unless one of a number of conditions is met (equal basis), including: - transfer to a white list jurisdiction; - the data subject has consented to the transfer; - transfer is for avoidance or mitigation of adverse action against the data subject; and	**YES (optional)** A *'data user'* may transfer personal data to a place outside Hong Kong when the data subject has consented in writing to the international transfer (s 33(2)(b)). Consent should be voluntarily given and not been withdrawn by the data subject in writing (International Transfer Guidance at 5).	**YES** Data may freely flow to a place designated by the PCPD as having been determined to have a *'law substantially similar to or serving the same purpose as'* the PDPO (a 'White List Jurisdiction') ((s 33(2)(a)). Such place is specified by notice in the Gazette (s 33(3)).	**YES** A data user may transfer data to jurisdictions which have not been white listed by PCPD where it has *'reasonable grounds for believing that there is in force in the place of transfer a law which is substantially similar to or serves the same purpose as'* the PDPO (s 33(2)(b). To satisfy such requirement, a data user is expected to undertake professional assessment and evaluation on its own of the data protection regime where the intended recipient is located. Such assessment should take into consideration various factors including the scope of application	**YES** *'Enforceable contract clauses*' may constitute *'reasonable precautions'* and *'due diligence'* to ensure that the data will not be transferred in contradiction with s 33 PDPO (s 33(2)(f); International Transfer Guidance, incl. Recommended Model Clauses at 7) In 2014 the PCPD published a set of Recommended Model Clauses for transfers outside Hong Kong which distinguish between 'core clauses' (obligations of the parties, liability and indemnity, settlement of disputes, termination) and 'additional clauses' (on third party rights and additional obligations of the transferee).	**YES** *'Adopting internal safeguards, policy and procedures for intra-group transfers'* can constitute *'reasonable precautions'* and *'due diligence'* to satisfy the conditions for transfers under s 33 PDPO (s 33(2)(f); International Transfer Guidance at 7).	**CONCEIVABLE** It is conceivable that the PCPD could consider if certification mechanisms, privacy seals and trust marks can constitute *'reasonable precautions'* and *'due diligence'* to satisfy the conditions for transfers under s 33 PDPO (s 33(2)(f)). The International Transfer Guidance (at 7) provides that *'non-contractual oversight and auditing mechanisms may be adopted to monitor the transferees' compliance with the data protection requirements under the Ordinance*'.	**NO** Hong Kong SAR is an APEC economy and the Office of the Privacy Commissioner for Personal Data is a participant to the CPEA. However, Hong Kong SAR has not yet expressed an intention to join the CBPR or PRP systems, hence the CBPR or PRP cannot be used to demonstrate compliance with the requirements of s 33.	**CONCEIVABLE** It is conceivable that the PCPD could consider if compliance with a highly regulated industry's code of practice would constitute *'reasonable precautions'* and *'due diligence'* to satisfy the conditions for transfers under s 33 PDPO. The International Transfer Guidance provides that *'non-contractual oversight and auditing mechanisms may be adopted to monitor the transferees' compliance with the data protection requirements under the Ordinance*' (at 7).	**STATUTORY EXEMPTIONS** Exemptions to the principles and conditions enacted in s33 apply in two categories of circumstances. - The prohibition against transfers of personal data to places outside Hong Kong does not apply where the personal data is exempted from Data Protection Principle 3 of the PDPO (i.e. use limitation requirement), such as prevention of crimes, legal proceedings, protection of health, statistics and research (where the resulting statistics or research does not identify the data subjects), and emergency situation (s 33(2)(e)).

- the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data concerned are given equivalent protection to that provided for by the Ordinance. Other exemptions can apply. **The Guidance on Personal Data Protection in Cross-border Data Transfer ('International Transfer Guidance')** adopted by the Hong Kong Privacy Commissioner in December 2014 serves as a practical guide for data users to implement s 33. The Privacy Commissioner has announced that it will publish an updated data transfer guidance in mid-2020 with enhanced user-friendliness and additional guidance towards organisational data users, especially the SMEs. *Note:* PDPO s 33 covers two situations: (i) transfers of personal data from Hong Kong to a place outside Hong Kong; and (ii) transfers of personal data between two other jurisdictions where the transfer is controlled by a Hong Kong data user.			of the data privacy regime, the existence of equivalent provisions of the DPPs in the Ordinance, the data subjects' rights and redress, the level of compliance and the data transfer restrictions. Mere subjective belief will not suffice. A data user must be able to demonstrate its grounds of belief are reasonable if challenged. Reference may be made to the methodology adopted by the Commissioner in compiling the White List (International Transfer Guidance at 4).	However, the Privacy Commissioner has announced that it will publish an updated data transfer guidance in mid-2020 with enhanced user-friendliness and additional guidance towards organisational data users, especially the SMEs, by introducing two sets of new recommended model clauses (including data transfers between 'data user and data user' as well as 'data user and data processor') for their adoption in formulating transfer agreements. The current clauses may be adapted and/or included in a data transfer agreement. Parties are advised to make adaptations or additions according to their own commercial needs. These clauses can be incorporated into a wider agreement such as an outsourcing agreement. The clauses may be adapted into a multi-party agreement.					- The transfer may also take place when the user has reasonable grounds for believing that, in all the circumstances of the case ((s 33(2)(d)): (i) the transfer is for the avoidance or mitigation of adverse action against the data subject; (ii) it is not practicable to obtain the consent in writing of the data subject to that transfer; and (iii) if it was practicable to obtain such consent, the data subject would give it. This exemption has a narrow application (International Transfer Guidance, at 6).
INDIA **(ACT IN FORCE)** **Information Technology Act, 2000 (IT Act), s 43A** **Information Technology Rules of the IT Act, 2011 (IT Rules), IT Rule on s 43A (Rule 7)** s 43A and IT Rule 7 apply exclusively to 'sensitive personal data'. Transfer of non-sensitive personal data is free. Specific localisation provisions may prevail in sectors including banking, telecom, and health.[1] Sensitive personal data or information may flow when: i) the information provider has consented to the transfer, or ii) the transfer is necessary for the performance of a contract. In any circumstances, the same level of data protection must apply to the data in the country of destination (Rule 7). Sensitive data or information consists of *'information relating to; (i) password; (ii) financial information (…) ; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of*	**YES (optional)** Sensitive personal data covered by the IT Rules may be transferred when the person has consented to the transfer, including third-party data processors. This rule applies to both domestic and international data transfers (Rule 7). In any circumstances the data subject's consent is not in itself a sufficient legal ground to transfer sensitive personal data to an overseas country, and the level of protection that will apply to that data in the country of destination must be the same as the level of protection provided for under the IT Rules (Rule 7).	**UNCERTAIN** In any circumstances sensitive personal data or information covered by the IT Rules may be transferred outside India only to a foreign country that *'ensures the same level of data protection that is adhered to by the body corporate as provided for under'* Rule 7. However, Rule 7 does not clarify by whom this assessment shall be made, nor the criteria by which the level of protection shall be assessed.	**UNCERTAIN** In any circumstances sensitive personal data or information covered by the IT Rules may be transferred outside India only to a foreign country that *'ensures the same level of data protection that is adhered to by the body corporate as provided for under'* Rule 7. However, Rule 7 does not clarify whether this assessment shall be made by the exporting organisation, nor the criteria by which the level of protection shall be assessed.	**UNCERTAIN** It is unclear whether contractual protections between the exporting and importing organisations would be considered as a valid means for a data exporter to demonstrate that the *'same level of data protection'* applies in the country of destination as in India in the meaning of Rule 7.	**UNCERTAIN** It is unclear whether the existence of binding corporate rules within a company group or a group of companies involved in joint economic activity would be considered as a valid means for a data exporter to demonstrate that the *'same level of data protection'* applies in the country of destination as in India in the meaning of Rule 7.	**UNCERTAIN** It is unclear whether national certifications delivered to overseas organisations would be considered as a valid means for a data exporter to demonstrate that the *'same level of data protection'* applies in the country of destination as in India in the meaning of Rule 7.	**NO** India is an observer to the CPEA but is currently not an APEC economy, hence the CBPR or PRP cannot be used to demonstrate compliance with the requirements of Rule 7.	**UNCERTAIN** It is unclear whether adherence by an overseas organisation to a locally approved code of conduct could be considered as a valid means for a data exporter to demonstrate that the *'same level of data protection'* applies in the country of destination as in India in the meaning of Rule 7.	**NO** No exception applies to the consent requirement or the requirement that the same level of data protection must apply in the country of destination in s 43A and IT Rule 7.

1 See Amber Sinha and Elonnai Hickok, 'Jurisdictional Report: India', in Regulation of Cross-Border Transfers of personal Data in Asia' (ABLI, 2018), p. 129.

the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise' (Rule 3).									
INDIA (BILL) **Data Protection Bill, Chapter VII (Restriction on transfer of personal data outside India), ss 33 and 34** *(introduced in Lok Sabha on December 10, 2019)* As in the framework currently in force, ss 33 and 34 would not apply to transfers of any personal data but to transfers of *'sensitive'*, but also to *'critical'* personal data for the purpose of processing. With regard to sensitive personal data, such data *'may be transferred outside India for the purpose of processing but shall continue to be stored in India'* (s 33(1)), and additional conditions apply (s 34(1), see next). Sensitive personal data is defined in s 3(36) and includes financial personal data. The list may be expanded by Government regulation. With regard to critical personal data, such data may be processed only in India, with exceptions (s 34(2)- see next). Critical personal data is undefined and may be notified as such by Government regulation. *Notes:* Personal data that is neither sensitive nor critical under the Data Protection Bill would be free to transfer (on the assumption that there is legal basis for the processing in the first place). This is in contrast with the transfer provisions in the original version of the Bill (2018), which prescribed specific measures for the transfer of personal data that was neither sensitive nor critical (s 40). Other requirements to store and/or process in India would apply in case of the cumulative application of localisation requirements for sectors including banking, telecom, and health (same as above). Localisation obligations were removed from the draft e-commerce policy in June 2019 (in anticipation of their displacement to the Data Protection Bill). More sectoral obligations to localise data are currently in draft, e.g. in the draft e-pharmacy rules.	**YES (required)** Sensitive personal data may only be transferred outside India when explicit consent is given by the data principal for such transfer (s 34(1)). As in the framework currently in force, consent is necessary but not sufficient for international transfers and additional measures apply (s 34(1)(a) or (b), see next). There are no legal consequences attached to the collection of the individual's consent with regard to the transfer of either critical personal data (which must in principle stay on shore) or of personal data which is neither sensitive nor critical (which is free to transfer, here again on the assumption that there is legal basis for the processing in the first place).	**YES** Different requirements apply depending on the nature of the personal data to be transferred. With regard to sensitive personal data, the Central Government, after consultation with the Data Protection Authority of India (DPAI), may allow the transfer to a country or, such entity or class of entity in a country or, an international organisation that provides an adequate level of protection (Bill, s 34(1)(b))— i) having regard to the applicable laws and international agreements, and ii) when such transfer shall not prejudicially affect the enforcement of relevant laws by authorities with appropriate jurisdictions. With regard to critical personal data, the Central Government may deem a transfer of critical personal data to be permissible to a country or, any entity or class of entity in a country or to an international organisation, when (Bill, s 34(2)(b))— i) it has previously found that the country, organisation, entity provides adequate protection, and ii) the transfer does not prejudicially affect the security and strategic interest of the State. However, the Bill does not clarify by whom this assessment shall be made, nor the criteria by which the level of protection shall be assessed.	**NO** Only the Central Government can make positive assessments based on either s 34(1)(b) or s 34(2)(b).	**YES** With regard to sensitive personal data only, such personal data may be transferred for the purpose of processing where the transfer is made *'pursuant to a contract approved by the Authority'* which makes the provisions for (s 34(1)(a)): i) effective protection of data principal's rights, including in relation to onward transfers, and ii) liability of the data fiduciary for harm caused due to non-compliance. Consent requirements still apply (s 34(1)).	**YES** *(For sensitive personal data only, s 34(1)(a))* Sensitive data may be transferred for the purpose of processing where the transfer is made *'pursuant to an intra-group scheme approved by the Authority'* which makes the provision for: i) effective protection of data principal's rights, including in relation to onward transfers, and ii) liability of the data fiduciary for harm caused due to non-compliance. Consent requirements still apply (s 34(1)).	**NO** The Bill does not mention the possibility for an exporting organisation to discharge the requirements in s 34 by providing safeguards through an approved certification mechanism, nor does it envisage the set-up of a privacy certification scheme in India. The closest reference to a certification scheme is in s 29(5) which envisions the assigning of a *'data trust score'* to *'Significant Data Fiduciaries'* (to be notified as such by the Government based on s 26(1)) to indicate the level of protection they provide. Though these could be given to overseas organisations operating in India it does not appear that they will be used in the context of cross border data transfers. The *'demonstrable verification mark'* envisioned in s 28(4)) (*'Social Media Intermediaries'* must provide an option to users registering from India or using their services in India for voluntary certification of their accounts, which will be marked with such a demonstrable certification marks) is unrelated to the implementation of data transfer provisions. Although it does not appear to be the intention, it is possible (at least conceptually) that certification of an organisation located in a third country to a privacy certification scheme in India, coupled with ad hoc contractual engagements between the parties, would be an admissible 'agreement' for the purpose of s 34(1)(a). It is also conceivable that an international or *ad hoc* bilateral agreement for certification could be concluded, which would later operate within s 34(1)(b)(i) (for sensitive data) or s 34(2)(b) (for critical data).	**NO** India is an observer to the CPEA but is currently not an APEC economy, hence the APEC CBPR or PRP systems could not be used to demonstrate compliance with s 34(1) of the Bill.	**UNCERTAIN** The Bill provides that the Authority shall, by regulations, specify codes of practice *'to promote good practice of data protection and facilitate compliance with the obligations of this Act'* (s 50(1)) and that codes of practice may include *'transfer of personal data outside India pursuant to s 34'* (s 50(6)(q)). However, the Bill does not envision the possibility for an exporting organisation to discharge the requirements in s 34(1) by providing safeguards through an approved code of practice. It is further uncertain (although not unconceivable) that compliance with a code of conduct in India by an organisation located in a third country, coupled with *ad hoc* contractual engagements between the parties, would be an admissible *'agreement'* for the purpose of s 34(1)(a).	**STATUTORY EXEMPTIONS** Different exemptions to data transfer provisions flow from Chapter VIII ('Exemptions'). - With regard to statutory exemptions, s36 provides that the data transfer restrictions in Chapter VII will not apply when it is necessary for the purposes of— - law enforcement; - legal proceedings; - exercise of any judicial function; - domestic purposes; or - journalistic purposes. - Critical personal data may further be transferred outside India to a person or entity providing health or emergency services where necessary for prompt action (s 34(2)(a)). Such transfer must be notified to the Authority (s 34(3)). **EXEMPTION BY THE CENTRAL GOVERNMENT** Bill s 37 ('BPO exemption') grants the power to the Central Government to exempt certain data processors from all or part of the Act (including Chapter VII) for the processing of personal data of data principals (individuals, ed.) outside India, pursuant to any contract entered into with any person outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law. **EXEMPTIONS BY THE AUTHORITY** With regard to sensitive personal data, the Authority may allow the transfer of sensitive personal data or class of sensitive personal data necessary *'for any specific purpose'* (s 34(1)(c)). Where the processing of any personal data (including sensitive or critical personal data) is *'necessary for research, archiving, or statistical purposes'*, the Authority may exempt such class of research, archiving, or statistical purposes from the application of any of the provisions of the Act (including s 34) as may be specified by regulations. The Authority must be satisfied that— (a) the compliance with the provisions of the Act shall disproportionately divert resources from such purpose; (b) the purposes of processing cannot be achieved if the personal data is anonymised;

									(c) the data fiduciary has carried out de-identification in accordance with the code of practice specified under s 50 and the purpose of processing can be achieved if the personal data is in de-identified form; (d) the personal data shall not be used to take any decision specific to or action directed to the data principal; and (e) the personal data shall not be processed in the manner that gives rise to a risk of significant harm to the data principal.
INDONESIA (LAW IN FORCE) **Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law), Art 26** **Regulation No.20 of 2016 of the Ministry of Communication and Information (MCI 20/2016), Arts 21 and 22** <u>Principle:</u> Electronic System Providers ('ESPs') may transfer data only with the individual's consent; and following 'coordination with the Ministry' (in the current case the Ministry of Communication and Information, or 'Kominfo'). The coordination requirement seems closer to a notification requirement than to a prior authorisation but sometimes regulatory scrutiny is applied.[2] **Government Regulation No.71 of 2019 (GR71), Arts. 20-21** *(has replaced Government Regulation No. 82 of 2012 (GR82) in October 2019)*: ESPs *'for Public Purposes'* may not process or store data outside Indonesia (with exceptions, i.e. unless the storage technology is not available in Indonesia (Art20) (subject to further implementing regulations). ESPs *'for Private Purposes'* may manage, process and/or store electronic system or electronic data inside or outside Indonesia (Art21(1)), subject to the obligation to ensure effective compliance with GR71 (Art21(2)) and to enable access to the data by the public authorities (Art21(3)) - (all of which subject to further regulations). ESPs that are deemed to have 'strategic electronic data' (for now undefined) must backup records to *'a certain data centre'* (Art99(3)). Regulatory guidance will be needed on the location of such data centres and whether 'Private ESPs' are included in the scope. The Financial Service Authority may adopt specific regulations relating to the transfers of personal data (Art21(4)).	**YES (required)** The written consent of the 'data owner' is required unless specific regulations apply (MCI 20/2016, Art 21(1)). Express opt-in is not explicitly required by Art 21(1) but is derived from MCI 20/2016, Art 1(4).	**UNCERTAIN** It is not known if the Ministry would assess the level of protection in certain countries (e.g. countries with data protection laws) in the context of the coordination provided in MCI 20/2016 Art 22.	**UNCERTAIN** It is not known if the assessment by the ESP that the data transfers take place to countries with a certain level of protection (e.g. countries with data protection laws) would be a positive factor if regulatory scrutiny were applied in the context of the coordination with the Ministry under MCI 20/2016 Art 22.	**UNCERTAIN** It is not known if the existence of *ad hoc* contractual provisions relating to the level of data protection applied by the importing organisation in the country of destination would be a positive factor in the context of ensuring coordination with the Ministry under MCI 20/2016 Art 22.	**UNCERTAIN** It is not known if the existence of BCRs or corporate rules that bind the importing organisation to ensure a certain level of data protection in the country of destination would be a positive factor in the context of ensuring coordination with the Ministry under MCI 20/2016 Art 22.	**UNCERTAIN** It is not certain if the existence of a certification scheme that would bind the importing organisation to ensure a certain level of data protection in the country of destination would be a positive factor in the context of ensuring coordination with the Ministry under MCI 20/2016 Art 22.	**NO** Indonesia is an APEC economy but as at April 2020 has not expressed an intention to join APEC CBPRs.	**UNCERTAIN** It is not certain if adherence of the importing organisation to a local Code of conduct that would ensure the application of a certain level of data protection in the country of destination would be a positive factor in the context of ensuring coordination with the Ministry under MCI 20/2016 Art 22.	**NO** No exception to consent or additional legal ground for transfers outside the territory of Indonesia applies.

2 Danny Kobrata, 'Jurisdictional Report: Indonesia', in Regulation of Cross-Border Transfers of personal Data in Asia' (ABLI, 2018), p. 151.

INDONESIA (BILL) **Data Protection Bill, Art 49** *(introduced in Parliament on January 28, 2020)* Overseas data transfers may in principle take place only in four series of circumstances presented as alternatives: - the level of protection in the country if destination is equal to, or higher than in the Act (Art 49(a)); - international agreements apply (Art 49(b)); - a contract offering appropriate safeguards is in place between the parties (Art 49(c)); - the data subject has consented to the transfer (Art 49(d)). These provisions will be later specified in a Government Regulation. *Notes:* The Data Protection Bill will not affect pre-existing data protection provisions in so far as they are not contradictory with the Bill and are not specifically regulated by it (Art 79). The localisation provisions in GR71 (above) and the requirement of coordination with the Ministry in Art 22(1) of MCI 20/2016 would therefore not be impacted by the Bill. The current version of the Bill does not institute a Data Protection Authority. It is not clear to which entity in the Government (beyond MCI) the implementation of the provisions of the future Law would be left.	**YES (optional)** Transfers may take place if *'there is written approval from the owner of the personal data'* (Art 49(d)). Consent can also be verbal, provided that it is recorded.	**CONCEIVABLE** Transfers may take place to a country or international organisation that '*has a personal data protection level that is equal to or higher than this law* ' (Art 49(a)). It is not certain, but conceivable if a public authority can make its own assessment and put countries on 'white lists' by way of consequence. This would however appear to be the original intention of the government. The Bill does not mention which entity in the government should make that assessment, and by which criteria. Such specifications would be provided in future regulations.	**CONCEIVABLE** Transfers may take place to a country or international organisation that has a *personal data protection level that is equal to or higher than this law*' (Art 49(a)) Since the Bill does not mention which entity should make that assessment, it is conceivable that the data exporter can make his own assessment. However, it is doubtful if such were the intention of the Government. The Bill also does not mention by which criteria this assessment should be made. Such specifications would be provided in future regulations.	**YES** The transfer may take place when a contract offering appropriate safeguards has been put in place between the Personal Data Controller and a third party outside the territory of the Unitary State of the Republic of Indonesia (Art 49(b)).	**CONCEIVABLE** It is not certain, but conceivable that BCRs would be covered by Art 49(b) providing that transfers can take place when there is a contract between the controller and an overseas third party, for instance when an intra-group agreement would support the BCRs.	**CONCEIVABLE** The current version of the Bill does not envisage the set-up of a certification scheme in Indonesia. It is uncertain, but conceivable that certification in Indonesia by an organisation located in a third country, coupled with *ad hoc* contractual engagements between the parties, would be an admissible contract for the purpose of Art 49(c). However, this does not rule out the possibility that an international or *ad hoc* bilateral agreement for certification could be concluded under Art49(b), which would later operate within Art 49(c).	**NO** Indonesia is an APEC economy but as at April 2020 has not expressed an intention to join APEC CBPRs.	**CONCEIVABLE** It is not certain, but conceivable that compliance with a Code of Conduct in Indonesia by an organisation located in a third country, coupled with *ad hoc* contractual engagements between the parties, would be an admissible *'agreement'* for the purpose of Art 49(c).	**ADDITIONAL LEGAL GROUND** Transfers may take place when *'there are international agreements between the countries'* (Art 49(b)).
JAPAN **Act on the Protection of Personal Information, 2016 (APPI), Art 24** Transfers of personal information by a *'Personal Information Handling Business Operator'* (PIHBO) in Japan to third parties located in overseas destinations are subject to obtaining the individual's consent, unless: - the country of destination has an equivalent level of protection (Art 24); - the recipient acts in conformity with a system established by standards prescribed by the Personal Information Protection Commission of Japan (PPC) (Art24); - one of a series of statutory exceptions apply (Art 23(1)). *Note:*	**YES (optional)** Consent is required, unless exceptions apply (Art 24). For consent to be valid, the data subject must be clearly informed that the personal information will be transferred to a third party in a foreign country, and be provided with all the information necessary to decide whether to consent (e.g. the foreign jurisdiction is identified or identifiable, or the circumstances in which such data transfer will take place have been clarified).	**YES** The PPC can whitelist a foreign country establishing a *'personal information protection system'* recognized to have equivalent standards to the standards in regard to the protection of an individual's rights and interests in Japan (APPI Art 24). In considering whether to put specific countries on a white list, the PPC makes a judgment relying on a series of '*judgmental standards'* for the assessment of this level of protection:[3] - there are statutory provisions or codes equivalent to those relating to the obligations of personal information handling business operators defined under the APPI, and the policies, procedures and systems to enforce compliance with these rules can be recognised; - there is an independent personal data protection authority, and the authority has ensured necessary	**NO** Only PPC can make positive assessments (i.e. put a foreign country on a white list) (APPI Art 24).	**YES** Transfers may take place on the basis of a contract if such a contract *'ensures, in relation to the handling of personal data by the person who receives the provision, the implementation of measures in line with the purpose of the provisions under APPI by an appropriate and reasonable method*' (APPI Art 24).	**YES** Transfers may take place on the basis of internal rules if such internal rules '*ensure, in relation to the handling of personal data by the person who receives the provision, the implementation of measures in line with the purpose of the provisions under APPI by an appropriate and reasonable method'* (Art24 APPI).	**YES** Transfers may take place on the basis of a certification if a person who receives the provision of personal data has obtained *'a recognition based on an international framework concerning the handling of personal information*' (which includes, but is not limited to CBPRs) (Art24 APPI). Transfers may take place if a personal information handling business operator is certified under the CBPRs (see next).	**YES** Japan's application to participate in CBPRs was endorsed by APEC and effective April 2014. JIPDEC was appointed as Japan's Accountability Agent in January 2016. PPC has recognized that CBPRs are a *'certification on the basis of an international framework regarding personal information handling'* that provide a level of protection equivalent to the APPI under Art24 (additional requirements apply to onward transfers of EU data).	**NO** Adherence to a code of conduct is not included in the examples of action which the recipient might take to be in conformity with a system established by reference to standards set by the PPC.	**STATUTORY EXEMPTIONS** Transfers may take place without the user's consent in specific circumstances listed in Art 23(1): (i) cases based on laws and regulations; (ii) cases *'in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent'*; (iii) cases *'in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent'*; and (iv) cases *'in which there is a need to cooperate in regard to a central government organisation or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the*

3 Profs Kaori Ishii and Fumio Shimpo, 'Jurisdictional Report: Japan, in Regulation of Cross-Border Transfers of personal Data in Asia' (ABLI, 2018), p. 182.

Transfers to others than *'third parties'* are not covered by Art 24 and consent requirements do not apply. Under the APPI, the following entities are deemed not to be third parties: - data processors; - a company that enters into a merger, a company split or a business transfer with the data controller; or - a company designated to jointly use the personal information with the controller.		enforcement policies, procedures and systems; - the necessity for a foreign country designation can be recognised as in Japan's national interest; - mutual understanding, collaboration and co-operation are possible; and, - establishing a framework to pursue mutual smooth transfer of personal information, while seeking the protection thereof, is possible. These standards were applied by the PPC in its decision of January 18, 2019, recognising that the European Union has established a *'personal information protection system'* based on standards equivalent to the standards of APPI in regard to the protection of an individual's rights and interests in Japan.							*performance of the said affairs*.'
MACAU SAR **Personal Data Protection Act (2005) (PDPA), Art 19 and 20** <u>Principle:</u> The transfer of personal data to a destination outside the MSAR may only take place subject to compliance with the PDPA and provided the legal system in the destination to which they are transferred ensures an adequate level of protection (Art19(1)). Transfers to 'non-adequate' destination countries may take place only if specific conditions are complied with (see next), and must be either notified to, or authorised by the Office of Personal Data Protection (OPDP).[4] The analysis carried out in the context of such procedures appears in decisions published on the OPDP's website.[5]	**YES (optional)** Unambiguous consent to data transfer may derogate to the absence of adequate protection in destination country (Art20(1)). Such transfer must in any case be notified to OPDP. There are, however, three cases in which the data subject's consent is not sufficient to transfer the data outside Macau: - the first two exceptions refer to sensitive data and to credit data (PDPA, Art 22(1)), whose processing is subject to the prior authorisation of the OPDP. Processing (including transfer) of these two categories of data is subject to prior authorisation by the OPDP, unless authorised by law; - the third exception is in relation to the interconnection or so-called combination of data (PDPA, Art 4, 1(10)), which is also subject to the prior authorisation of OPDP.	**YES** The public authority may decide that the legal system in the destination to which they are transferred ensures an adequate level of protection (Art 19(2) and (3)). The adequacy of the level of protection shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations. Particular consideration shall be given to: - the nature of the data, - the purpose and duration of the proposed processing operation or operations, - the place of origin and place of final destination, - the rules of law, both general and sectoral, in force in the destination in question, and - the professional rules and security measures which are complied with in that destination (Art19(2)). Such transfer need not be authorised by, or notified to OPDP.	**NO** It is for the public authority to decide whether a legal system ensures an adequate level of protection (Art19(3)).	**YES** The OPDP may authorise transfers where the controller adduces *'adequate safeguards', 'particularly by means of appropriate contractual clauses*' (Art20(2)). Such transfer must be authorised by OPDP.	**CONCEIVABLE** It is uncertain, but not unconceivable that the OPDP could take the decision to authorize a transfer based on the consideration that BCRs or internal rules would constitute *'adequate safeguards'* in the meaning of Art20. Such transfer would have to be authorised by OPDP.	**CONCEIVABLE** It is uncertain, but not unconceivable that the OPDP could take the decision to authorise a transfer based on the consideration that Certification Schemes would constitute *'adequate safeguards'* in the meaning of Art20(2). Such transfer would have to be authorised by OPDP.	**NO** Macau SAR is not an APEC economy, hence cannot currently join CBPRs or PRP.	**CONCEIVABLE** It is uncertain, but not unconceivable that the OPDP could take the to authorise a transfer based on the consideration that a Code of conduct would constitute *'adequate safeguards'* in the meaning of Art20(2). Such transfer would have to be authorised by OPDP (Art20(2)).	**STATUTORY EXCEPTIONS** A transfer to a destination in which the legal system does not ensure an adequate level of protection *'may be allowed'* where (PDPA Art 20(1)): (1) it is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; (2) it is necessary for the performance or conclusion of a contract concluded or to be concluded in the interests of the data subject between the controller and a third party; (3) it is necessary or legally required on important public interest grounds, or for the establishment, exercise of defence of legal claims; (4) it is necessary in order to protect the vital interests of the data subject; (5) it is made from a register which according to laws or administrative regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest. Such transfers must be notified to OPDP.
MALAYSIA **Personal Data Protection Act (PDPA) 2010, s 129** Data transfers outside Malaysia may in principle take place only to places specified by the Minister	**YES (optional)** Consent may operate as an exception to the requirement that transfers may take place only to places specified by the Minister (s 129(2)(a)).	**YES** The Minister, upon the recommendation of the Commissioner, may specify any place outside Malaysia to where data may freely flow, where: a) there is in that place in force any *'law which is substantially similar*	**NO** Only the Minister can make related specifications (s 129(1)).	**YES (implicit)** The data user should *'take all reasonable precautions and exercise all due diligence'* to ensure that the data will be adequately protected overseas, which implicitly refers to the conclusion	**CONCEIVABLE** It is not certain, but conceivable that BCRs and internal rules are considered as *'reasonable precautions'* and measures of *'due diligence'* in the meaning of s 129(2)(f).	**CONCEIVABLE** It is not certain, but conceivable that certification in Malaysia by an organisation located in a third country to a privacy scheme or obtaining a privacy mark may constitute *'reasonable precautions'* and measures of *'due diligence'* in	**NO** Malaysia is an APEC economy but as at April 2020 has not expressed an intention to join the CBPR system.	**CONCEIVABLE** It is not certain, but conceivable that adherence of the overseas recipient to a code of conduct may be considered as *'reasonable precautions'* and measures of *'due diligence'* in the meaning of PDPA s 129(2)(f).	**EXEMPTION BY AUTHORITY** A 'data user' or 'class of users' may be exempted from all or part of the PDPA (including s 129) by decision of the Minister following the prior opinion of the Commissioner (S46(1)). **STATUTORY EXCEPTIONS**

4 On the operation of these procedures, see Graça Saraiva, 'Jurisdictional Report: Macau SAR, in Regulation of Cross-Border Transfers of personal Data in Asia' (ABLI, 2018), p. 202.
5 For instance, Opinion No.0016/P/2018/GPDP on the establishment of the CTM (Macau Telecommunications Company) (HK) Data Centre and the transfer of data from Macao to Hong Kong and the respective notification and authorisation procedures.

where there is in force any law which is substantially similar to, or that serves the same purposes as the PDPA or which ensures an adequate level of protection which is at least equivalent to the level of protection afforded by PDPA. 'The Minister' refers to the Minister *'charged with the responsibility for the protection of personal data'*, currently the Communications and Multimedia Minister (PDPA s 4). Transfers by a 'Data User' in Malaysia to other destinations may take place only if: - The data subject has consented to the transfer; - The data user has taken reasonable precautions and exercised due diligence; or - Statutory or regulatory exemptions apply. *Notes:* On 14 February 2020 the Malaysian Personal Data Protection Commissioner ('Commissioner') has issued a Public Consultation Paper on review of the PDPA. One of the suggestions proposed is for removal of the provisions in s 129 which provide for the issuance of a whitelist by the Minister. As part of the ongoing review exercise, the Commissioner is considering issuing a guideline to address the mechanism and implementation of cross border transfers (Proposed Improvement Suggestion Nr.13). If implemented, it is unclear whether transfers which comply with the transfer mechanisms set out in the said guidelines will be recognised as permissible under the PDPA.		*to this Act, or that serves the same purposes as PDPA'*; or (b)that place ensures an adequate level of protection in relation to the processing of personal data which is '*at least equivalent to the level of protection afforded by PDPA'*. (s 129(1)) *'The Minister'* refers to the Minister *'charged with the responsibility for the protection of personal data'* (S4 PDPA), currently the Communications and Multimedia Minister. *Note:* The Commissioner is considering removal of the whitelist provisions above as part of the ongoing PDPA review exercise.		of contracts (s 129(2)(f)). Contracts are further mentioned as such safeguards in sectoral Codes of conduct approved by the Commissioner.		the meaning of PDPA s 129(2)(f).		PDPA s 23 describes the conditions under which codes of conduct may be drafted and registered with the Commissioner but these provisions are unrelated to those relating to data transfers.	Transfers of personal data may take place to other non-adequate destinations if (s 129(3)(b) to (h)): (b) the transfer is necessary for the performance of a contract between the data subject and the data user; (c) the transfer is necessary for the conclusion or performance of a contract between the data user and a third party which—(i) is entered into at the request of the data subject; or (ii) is in the interests of the data subject; (d) 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; (e) the data user has reasonable grounds for believing that in all circumstances of the case— (i) the transfer is for the avoidance or mitigation of adverse action against the data subject; (ii) it is not practicable to obtain the consent in writing of the data subject to that transfer; and (iii) if it was practicable to obtain such consent, the data subject would have given his consent; (…) (g) the transfer is necessary in order to protect the vital interests of the data subject; or (h) the transfer is necessary as being in the public interest in circumstances as determined by the Minister.
NEW ZEALAND (ACT IN FORCE) **Privacy Act 1993, Part 11A (Transfer of Personal Information outside New Zealand), s 114B** International transfers are permitted, as long as the legal requirements in the privacy principles and appropriate conditions for privacy protection are observed. However, in exceptional circumstances the Privacy Commissioner may prohibit a transfer to another State when: - The personal information has been received from another State and will be transferred to a third State where it will not be subject to a law providing comparable safeguards to the Privacy Act; and - The transfer would be likely to breach the basic principles of national application set out in the OECD Guidelines.	**NO** Consent is neither optional nor required, and would not currently appear to waive the requirements of existing privacy safeguards in the country of destination. The Privacy Act does not mention it, nor the Privacy Commissioner's Fact Sheet on Part 11A.	**NO** The Privacy Act does not provide for the possibility to adopt *'white lists'*. However, the Commissioner may prohibit a transfer *'if the information has been, or will be, received in New Zealand from another State and is likely to be transferred to a third State where it will not be subject to a law providing comparable safeguards to this Act*' and the transfer would be likely to lead to a contravention of the basic principles of national application. There is no formal process for recognising the receiving jurisdiction meets standards of comparability at present.	**NO** The Privacy Act does not cater for this possibility.	**YES** Contractual provisions governing handling of personal data are common although they are not mentioned in the Privacy Act itself. The EU model clauses are referred to in the Fact Sheet on Part 11A of the Privacy Act 1993 as *'associated schemes established under the international instruments which, although not being privacy laws of a State, may nonetheless provide comparable safeguards*.'	**YES** BCRs are not mentioned in the Privacy Act itself but they are referred to in the Fact Sheet on Part 11A of the Privacy Act 1993 as *'associated schemes established under the international instruments which, although not being privacy laws of a State, may nonetheless provide comparable safeguards.'*	**UNCERTAIN** Regulatory guidance does not explicitly refer to trust marks and privacy seals as *'associated schemes established under the international instruments which, although not being privacy laws of a State, may nonetheless provide comparable safeguards*.' The Privacy Trustmark in New Zealand further has no legal standing and is not articulated with Part 11A of the Privacy Act, although it might be used by a foreign agency as a means to provide evidence about its good privacy practices.	**NO** New Zealand is an APEC economy but as at April 2020 has not expressed an intention to join APEC CBPRs.	**UNCERTAIN** Regulatory guidance does not explicitly refer to Codes of conduct as *'associated schemes established under the international instruments which, although not being privacy laws of a State, may nonetheless provide comparable safeguards*' in the meaning of Part 11A of the Privacy Act.	**STATUTORY LIMITATION (TO POWER OF COMMISSIONER)** The Commissioner may not prohibit a transfer if it is (s 114B(3)): (a) required or authorised by or under any enactment; or (b)required by any convention or other instrument imposing international obligations on New Zealand. This same policy should follow through to the Privacy Bill (Part 8 of the Privacy Bill: Prohibiting onward transfer of personal information received in New Zealand from overseas).

The Fact sheet on Part 11A of the Privacy Act published by the Commissioner sets out certain matters that the Commissioner must consider in exercising the discretion to prohibit a transfer, including by showing *'legal regimes that might be thought likely to offer comparable safeguards to the Privacy Act'*. **Privacy Act, s 3(4)** *(applicable to e.g. cloud storage overseas).* Where an agency holds information— (a) solely as agent; or (b) for the sole purpose of safe custody; or (c) for the sole purpose of processing the information on behalf of another agency— and does not use or disclose the information for its own purposes, the information shall be deemed to be held by the agency on whose behalf that information is so held or, as the case may be, is so processed.									
NEW ZEALAND (BILL) **Privacy Bill, Information Privacy Principle 12 (IPP 12)** IPP 12 is to be combined with IPP 11 *('Limits of disclosure of personal information').* If data that may be legally transferred based on IPP11 is transferred to an overseas recipient, the *'exporting agency'* would need to satisfy one of the criteria set out in IPP 12(1): - the individual concerned authorises the disclosure, - the foreign person or entity is carrying on business in New Zealand, and the agency believes, on reasonable grounds, that the foreign person or entity is subject to the bill - the agency believes on reasonable grounds that: i) the foreign person or entity is *'subject to privacy laws that, overall, provide comparable safeguards'* to those in the bill; ii) the foreign person or entity is a participant in a prescribed binding scheme, or is subject to privacy laws of a *'prescribed country'*; or iii) the foreign person or entity must protect the information in a way that, overall, provides *'comparable safeguards'* to those in the bill. **Privacy Bill, Part 8** *('Prohibiting onward transfer of personal information received in New Zealand from overseas')* replicates the provisions of s 114B relating to transfer prohibition notices in the current Privacy Act (above).	**YES (optional)** An agency A may disclose personal information to a foreign person or entity B if the individual concerned *'authorises the disclosure to after being expressly informed by A that B may not be required to protect the information in a way that, overall, provides comparable safeguards to those in this Act'* (IPP 12(1)(a)). There is no formal process for recognising if the receiving jurisdiction meets standards of comparability at present.	**YES** An agency may disclose personal information to a foreign person or entity if it believes on reasonable grounds that the recipient is *'subject to privacy laws of a prescribed country'* (IPP 12(1)(e)). *'Prescribed country'* means a country specified in regulations made under s 212B. The Minister may recommend the making of such regulations only if he/she is *'satisfied that the countries have privacy laws that, overall, provide comparable safeguards to those in this Act'.*	**YES** An agency may disclose personal information to a foreign person or entity if it believes on reasonable grounds that the recipient is subject to *privacy laws that, overall, provide comparable safeguards to those in'* the Privacy Act (IPP12(1)(c)).	**YES** An agency may disclose personal information to a foreign person or entity if it believes on reasonable grounds that the recipient is *'required to protect the information in a way that, overall, provides comparable safeguards to those in this Act, for example, pursuant to an agreement'* entered into between agency and recipient) (IPP 12(1)(f)).	**YES** An agency may disclose personal information to a foreign person or entity if it believes on reasonable grounds that the recipient is *'required to protect the information in a way that, overall, provides comparable safeguards to those in this Act'* (IPP12(1)(f)) BCRs would likely qualify as such *'comparable safeguards'* as an extension of current regulatory guidance (above).	**YES (implicit)** Adherence of the overseas recipient to a recognised certification scheme could be considered as a part of considering whether the foreign person or entity is *'required to protect the information in a way that, overall, provides comparable safeguards to those in the Privacy Act'* (IPP12(1)(f)).	**CONCEIVABLE** New Zealand is an APEC economy but as at April 2020 has not expressed an intention to join APEC CBPRs. However, IPP12 provides for the New Zealand Government to prescribe binding cross-border privacy schemes such as CBPRs as a *'prescribed binding scheme'* under the Privacy Act. If New Zealand prescribes a binding scheme under the Privacy Bill this will be done through **IPP12(1)(d):** An agency may disclose personal information to a foreign person or entity if it believes on reasonable grounds that the recipient is a participant of a *'binding scheme*, ie *'an internationally recognised scheme in which the participants agree to be bound by a) specified measures for protecting personal information that is collected, held, used, and disclosed; and b) mechanisms for enforcing compliance with those measures*'. *'Prescribed binding scheme'* means a binding scheme specified in regulations made under section 212A by Order of the Governor-General.	**CONCEIVABLE** It is possible that voluntary adherence of the recipient to a Code of conduct could contribute to agency believing on reasonable grounds that the foreign person or entity is subject to *'comparable safeguards'* in the meaning of IPP12(1)(f)	**ADDITIONAL LEGAL GROUND** An organisation A may disclose information to organisation B if *'A believes on reasonable grounds that B is subject to the Privacy Act, when it is carrying on business in New Zealand*' (i.e. exception applies when for the purposes of the Bill both agencies are New Zealand agencies anyway) (IPP12(1)). **STATUTORY EXEMPTIONS** No restriction applies to overseas data transfers if the disclosure of the information is necessary (IPP12(2)): (i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or (ii) for the enforcement of a law that imposes a pecuniary penalty; or (iii) for the protection of public revenue; or (iv) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or (f) that the disclosure of the information is necessary to prevent or lessen a serious threat to— (i) public health or public safety; or (ii) the life or health of the individual concerned or another individual; and: it is not reasonably practicable in the circumstances to comply with the IPP 12 requirements.

									STATUTORY LIMITATION (TO POWER OF COMMISSIONER) The same policy as in S114B(3) (above) should follow through to Part 8 of the future law *('Prohibiting onward transfer of personal information received in New Zealand from overseas')* to the effect that the Commissioner may not prohibit a transfer if it is: (a) required or authorised by or under any enactment; or (b)required by any convention or other instrument imposing international obligations on New Zealand.
PHILIPPINES **Data Privacy Act of 2012 (DPA), s 21** There are no specific provisions on international transfers in the DPA but S 21 of the DPA (Accountability Principle) allows for data sharing outside the Philippines' borders as long as the lawful criteria in ss 12 and 13 are met, and the general privacy principles are followed. s 21 provides that *'any controller is responsible for personal information under its control and custody, including information that has been transferred to third parties for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation'.* Moreover, regarding data transfer for processing s 21(a) requires the controller to use '*contractual or other reasonable means to provide a comparable level of protection while information is being processed by a third party'.* Proposed amendments to s 21 in House Bill No. 5612 introduced in the House of Representatives on 25 Nov. 2019 do not modify the legal regime applicable to international transfers (but for additional transparency requirements on transfers). **Implementing Rules and Regulations (IRRs), Rule IV:** A specific provision applies to data sharing (s 20, *General Principles for Data Sharing*). The provision applies to data sharing in the private sector and between government agencies. **IRRs, Rule X:** Specific provisions apply to outsourcing and subcontracts (s 43 and s 44).	**YES (optional)** Data subject's consent is neither required nor mentioned as a method for the data controller to discharge its responsibility *'for personal information under its control and custody'* in the meaning of s 21. However, the lawful criteria under ss 12 and 13 apply with equal force to data sharing, whether within or outside the Philippines. Consent is an example of such lawful criteria. Hence, it may be considered as an option to transfer data overseas. Moreover, Rule 20(b) of the IRRs (*General Principles for Data Sharing)* provide that *'data sharing shall be allowed in the private sector if the data subject consents to data sharing*', and other conditions apply (data sharing shall be covered in a data sharing agreement). Consent for data sharing shall be required even when the data is to be shared with an affiliate or mother company, or similar relationships (s 20(b)(1)).	**NO** Neither DPA nor IRRs mention the level of data protection in an overseas destination as a relevant factor for a controller to assess its responsibility for transferring personal information under its control and custody, in the meaning of s 21. Proposed amendments to s 21 in House Bill No. 5612 introduced in the House of Representatives on 25 November 2019 do not modify the legal regime applicable to international transfers.	**NO** Neither DPA nor IRRs mention the level of data protection in an overseas destination as a relevant factor for a controller to assess its responsibility for transferring personal information under its control and custody, in the meaning of s 21. Proposed amendments to s 21 in House Bill No. 5612 introduced in the House of Representatives on 25 November 2019 do not modify the legal regime applicable to international transfers.	**YES (implicit)** Neither DPA nor IRRs explicitly provide that the implementation of contractual safeguards can discharge the responsibility of an organisation for exporting '*personal information originally under its custody or its control*'. However, this is subsumed in s 21 DPA and S44 IRR that specify data protection requirements for Outsourcing Agreements and contemplate both local and international data sharing. **s 20(b)(2) IRRs** prescribes that data sharing '*for commercial purposes, including direct marketing, shall be covered by a data sharing agreement.'* The data sharing agreement shall establish adequate safeguards for data privacy and security, and uphold rights of data subjects. It shall be subject to review by the Commission, on its own initiative or upon complaint of data subject. Regarding data transfer for processing **s 21(a) DPA** requires the controller to use '*contractual or other reasonable means to provide a comparable level of protection while information is being processed by a third party'.*	**CONCEIVABLE** It is conceivable, but not confirmed that the implementation of BCRs can discharge the responsibility of an organisation under s 21 DPA for exporting '*personal information originally under its custody or its control*', including for processing. It is conceivable, but not certain that BCRs for processors could qualify as *'reasonable means'* under s 21(a) which provides that controller should use '*contractual or other reasonable means to provide a comparable level of protection while information is being processed by a third party'.*	**CONCEIVABLE** It is conceivable, but not confirmed under either DPA or IRRs that the obtaining of (either local or overseas) certification can help an organisation discharge its responsibility for exporting '*personal information originally under its custody or its control*', and so *'including information that has been transferred to third parties for processing'.* Likewise, it is conceivable, but not certain that the obtaining of certification could qualify as *'reasonable means to provide a comparable level of protection while information is being processed by a third party'* under s 21(a).	**YES** On September 20, 2019, the Philippines National Privacy Commission announced it has filed its notice of intent to join the APEC CBPR system. The Joint Oversight Panel approved the Philippines' application to join the system on March 9, 2020. NPC would later recognise that CBPRs are part of the mechanisms by which the controller use '*reasonable means to provide a comparable level of protection while information is being processed by a third party'* (s 21(a)).	**CONCEIVABLE** It is conceivable, but not confirmed under the Act or the IRRs if adherence of a data recipient to a code of conduct can discharge the responsibility of the exporting organisation for '*personal information originally under its custody or its control*', and so *'including information that has been transferred to third parties for processing'.* DPA s 7(j) provides that the NPC has the function to *'review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers*.' However, it does not make a reference to the role which such codes might play in relation to s 21.	**ADDITIONAL LEGAL GROUND** No exception is provided to the accountability principle in s 21. However, s 20(a) IRRs *(General principles for data sharing)* provides that data sharing shall be allowed *'when it is expressly authorized by law*', provided that *'there are adequate safeguards for data privacy and security, and processing adheres to principle of transparency, legitimate purpose and proportionality*. *Mutatis mutandis* this provision is applicable to the transfer of personal data out of the Philippines when such transfer is provided by law.
SINGAPORE **Personal Data Protection Act (PDPA) 2012, s 26** *Transfer Limitation Obligation ('TLO')*: An organisation shall not transfer any personal data to a country or territory outside	**YES (optional)** The requirements of s 26 may be satisfied if the transferring organisation obtains the individual's consent to the effect of transferring the data (Reg 9(3)(a)).	**CONCEIVABLE** The general rule is that the exporting organisation has taken *'appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data in that country or territory outside Singapore (if any) is bound by legally enforceable obligations to*	**YES** Assessment of the standard of protection in the country or territory of destination may be done by the exporting organisation itself. Regarding Cloud Services, for instance, the PDPC Guidelines has	**YES** *'Legally enforceable obligations'* that provide a level of protection comparable to PDPA include obligations that can be imposed on the recipient by *'a contract'* (Reg 10(1)(b)).	**YES** *'Legally enforceable obligations'* that provide a level of protection comparable to PDPA in the meaning of s 26 include obligations that can be imposed on the recipient by *'binding corporate rules*.' (s 26), which may be adopted in '*instances where a*	**YES (implicit)** *'Legally enforceable obligations'* that provide a level of protection comparable to PDPA in the meaning of s 26 include obligations that can be imposed on the recipient by the local law of the country of destination, a contract, binding corporate rules or *'any*	**YES** On 20 February 2018 Singapore has joined the APEC CBPR and PRP systems. On 17 July 2019 the Infocomm Media Development Authority (IMDA) was appointed as Singapore's Accountability Agent.	**CONCEIVABLE** **'***Legally enforceable obligations'* that provide a level of protection comparable to PDPA in the meaning of s 26 include obligations that can be imposed on the recipient by the local law of the country of destination, a contract, binding corporate rules or *"any*	**STATUTORY EXEMPTIONS** The transfer of personal data to organisations that do not provide a standard of protection to personal data that is comparable to the protection under PDPA in the meaning of s 26 is allowed when:

Singapore except in accordance with requirements prescribed under PDPA to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under PDPA. **Personal Data Protection Regulations 2014, Part III, Regulations (Regs 8-10)** **Personal Data Protection Commission (PDPC) Advisory Guidelines (AG) on Key Concepts in the PDPA, Chapter 19** For the purposes of s 26 of PDPA, a transferring organisation must take appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data in that country or territory outside Singapore (if any) is bound by legally enforceable obligations (in accordance with PDPA Reg.10) to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the Act. **PDPC AG on Key Concepts in the PDPA, Chapter 8** ('Cloud Services') *(revised 9 October 2019)* An organisation that engages a Cloud Service Provider (CSP) as a data intermediary ('processor', ed.) to provide cloud services is responsible for complying with the TLO in respect of any overseas transfer of personal data in using the CSP's cloud services. This is regardless of whether the CSP is located in Singapore or overseas.	Consent cannot be used to waive the requirement of existing privacy safeguards in the country of destination. Reg 9(4) provides that an individual is not taken to have consented to the transfer of the individual's personal data to a country or territory outside Singapore if — a) The individual was not, before giving his consent, given a reasonable summary in writing of the extent to which the personal data to be transferred to that country or territory will be protected to a standard comparable to the protection under the Act; b) the transferring organisation required the individual to consent to the transfer as a condition of providing a product or service, unless the transfer is reasonably necessary to provide the product or service to the individual; or c) The transferring organisation obtained or attempted to obtain the individual's consent for the transfer by providing false or misleading information about the transfer, or by using other deceptive or misleading practices.	*provide to the transferred personal data a standard of protection that is at least comparable to the protection under the Act'* (s 26). The Minister for Communications and Information (MCI) could make regulations and PDPC could issue Advisory Guidelines setting out the criteria for assessment. However, the PDPA does not literally provide for the adoption of white lists and such would in any case not be the intention.	clarified that an organisation *'should ensure that any overseas transfer of personal data as a result of engaging a CSP will be done in accordance with the requirements under the PDPA',* namely, the organisation could ensure that the CSP it uses *'only transfers data to locations with comparable data protection regimes',* or has legally enforceable obligations to ensure a comparable standard of protection for the transferred personal data (PDPC Guidelines, Chapter 8, Para. 8.4).	- Any contract must (Reg 10(2); PDPC AG, 19.2): i) require the recipient to '*provide to the personal data transferred to the recipient a standard of protection that is at least comparable to the protection under the PDPA'*; and ii) specify *'the countries and territories to which the personal data may be transferred under the contract*'. - In setting out contractual clauses that require the recipient to comply with a standard of protection *'at least comparable to the protection under the PDPA,'* a transferring organisation should minimally set out protections with regard to *'areas of protection*' listed in a table provided in PDPC AG (Chapter 19.5). - Chapter 8 of PDPC AG ('Cloud Services'): an organisation may be considered to have taken appropriate measures to comply with the TLO by ensuring that (…) *'the recipients (e.g. data centres or sub-processors) in these locations are legally bound by similar contractual standards.'*[6]	*recipient is an organisation related to the transferring organisation and is not already subject to other legally enforceable obligations in relation to the transfer'* (Reg 9). BCRs must (Reg. 10-3; PDPC AG, Chapter 19.2): i) require every recipient of the transferred personal data to provide to the personal data transferred to the recipient a standard of protection that is at least comparable to the protection under the PDPA; and ii) specify the recipients of the transferred personal data to which the BCRs apply; the countries and territories to which the personal data may be transferred; and the rights and obligations provided by the BCRs. BCRs may only be used for recipients that are related to the transferring organisation (Reg.13(3)(c)). 'Recipients' are defined in Reg.13(3)(d)).	*other legally binding instrument'*. Certification could be among these legally binding instruments. PDPC has recently amended the PDPA Regulations to recognise that a recipient organisation holding a 'specified certification', including certification to the APEC CBPR and PRP Systems (see next column), would meet such legally enforceable requirements under s 26 PDPA. Regarding Cloud Services, the PDPC Guidelines (Chapter 8, Para 8.7) provide that where the contract between an organisation and its CSP does not specify the locations to which a CSP may transfer the personal data processed and leaves it to the discretion of the CSP, the organisation may be considered to have taken appropriate steps to comply with the Transfer Limitation Obligation by ensuring that: (a) the CSP based in Singapore is certified or accredited as meeting relevant industry standards, and (b) the CSP provides assurances that all the data centres or sub-processors in overseas locations that the personal data is transferred to comply with these standards. PDPC has plans to recognise APEC CBPR and PRP, as well its national Data Protection TrustMark (DPTM) certification as data transfer mechanisms under the PDPA.	PDPC has also recently amended the PDPA Regulations to recognise that a recipient organisation holding a 'specified certification', i.e. the APEC CBPR System, and the APEC PRP System would be taken to have met such legally enforceable requirements. Such certification therefore is compliant with s 26 PDPA.	*other legally binding instrument".* It is conceivable that codes of conduct could constitute such *'legally binding instruments'* under s 26 PDPA.	- the transfer is necessary for the performance of a contract between the individual and the transferring organisation, or to do anything at the individual's request with a view to the individual entering into a contract with the transferring organisation (Reg 9(3)b); - the transfer is necessary for the conclusion or performance of a contract between the transferring organisation and a third party which is entered into at the individual's request (Reg. 9(3)(c) or which a reasonable person would consider the contract to be in the individual's interest (Reg9(3)(d)); - the personal data is data in transit (Reg 9(3)(f)); or - the data is publicly available in Singapore (Reg 9(3)(g)); or - the transfer of personal data is necessary for a use or disclosure in certain situations where the consent of the individual is not required under the PDPA (Third and Fourth Schedule), such as use or disclosure necessary to respond to an emergency that threatens the life, health or safety of an individual. The transferring organisation will also need to take reasonable steps to ensure that the data will not be 'used or disclosed by the recipient for any other purpose' (Reg 9(3) and PDPC AG, Chapter 19). **EXEMPTION BY THE AUTHORITY** PDPC may, on the application of any organisation, by notice in writing exempt the organisation from any requirement prescribed pursuant to s 26(1) in respect of any transfer of personal data by that organisation (s 26(2) PDPA). An exemption granted under s 26(2) may be granted subject to such conditions as the PDPC may specify in writing and may be revoked at any time by the PDPC. Organisations should provide exceptional and compelling reason(s), accompanied with evidence of the reason(s) why the organisation is unable to comply with the PDPA provision(s).
SOUTH KOREA **Personal Information Protection Act No. 16930 (PIPA), Art 17** *(amended 4 February 2020)* PIPA contains the baseline provisions on data transfers from South Korea. It is complemented by the **Enforcement Decree of PIPA** No. 28355, Oct. 17, 2017 *(to be further amended).* **Act on the Promotion of Information and Communications Network Utilization and Data Protection** ('**Network Act'**), **Art 63** *(amended 4 February 2020)*	**YES (required)** **PIPA, Art 17** Consent is required to transfer personal data to any third party, whether locally or overseas (Art 17(1)). Specific consent must be sought for transferring data overseas (Art 17(3)). Conditions for obtaining valid consent are prescribed in PIPA (Arts 17(2), 22). **Network Act, Art 63** *(to be displaced and renumbered as PIPA, Art 39(12) on 5 August 2020):* ICSPs must obtain data subject's	**NO** Neither the current framework on data transfers (in PIPA or Network Act), nor the amended Acts refer to 'white lists', 'adequacy findings', etc. However, it is anticipated that the newly amended PIPA could be further amended to cater for this possibility in the future.	**NO** Neither the current nor the amended framework cater for this possibility.	**NO** Neither the current nor the amended Acts explicitly refer to contracts for data transfers. However, the interpretation is that contracts are necessary: The **PIPA** does not require the data exporter to enter into a contract, nor does it specifically mention the use of contracts for overseas data transfers, but it prohibits the importer from *'entering into a contract which would not be compliant with applicable laws.'* The **Network Act** requires certain items to be included in a contract for the transfer of personal information, irrespective of the	**NO** Neither the current nor the amended framework refer to BCRs.	**NO** Neither the current data transfer provisions in PIPA and Network Act, nor Art 63 Network Act (eventually Art 39(12) PIPA) expressly refer to certification mechanisms for data transfers. The amendment bill to the Network Act originally provided that consent requirements would be waived *'where the overseas recipient of the transfer has been certified under the Personal Information Management System ('PIMS') certification scheme [now 'ISMS-P'] or other certification designated by KCC'* but this reference was eventually rejected	**YES** The participation of South Korea in the CBPR System was approved on June 12, 2017. KISA was appointed CBPR Accountability Agent in January 2020 but KISA's CPBR checklist has not been published. Plans to articulate PIMs (now ISMS-P) and CBPRs were announced. However, these plans have become unclear since reference to the ISMS-P scheme (and certification generally) in relation to cross border data transfers was eventually removed from the Bill.	**NO** Neither the current nor the amended framework refer to codes of conduct for transfers at this stage.	**STATUTORY EXEMPTIONS** Consent requirements are exempted for overseas data transfers only in specific circumstances listed by statute. For now, explicit exceptions exclusively pertain to 'controller-processor' transfers (for 'entrustment of management or storage') which are carried out by ICSPs and Extended ICSPs under the Network Act. Under Network Act Art 63(2) consent is not required where the delegation by the ICSP is 'necessary for the performance of the contract on the provision of information communication

6 See Decision [2019] SGPDPC 22 (Case No DP-1708-B1027, Spize Concepts Pte Ltd), 4 July 2019, Paras. 25 and ff.

The Network Act makes specific provisions relating to data transfers by Internet Content Service Providers (ECSPs) and recipients of data collected by ICSPs (Extended ICSPs).7 It is complemented by the **Enforcement Decree of Network Act** (esp. Art 67). Data transfer provisions in other statutes (e.g. Credit Information Act, Location Information Act) may also apply. The overarching principle to all data transfer provisions is that express user consent is required to transfer personal data to third parties located overseas. Limited exceptions to consent requirements apply in specific circumstances provided by statute, specifically in relation to overseas controller-processor transfers for delegation of processing (outsourcing). *Notes*: - On 4 February 2020 major amendments to PIPA, Network Act, and Credit Information Act were promulgated *(entry into force: 5 August 2020).* The amended PIPA will include a new Chapter 6 *(Special Provisions for the Processing of Personal Information by 'ICSPs' and 'extended ICSPs')* importing the data protection provisions of the Network Act which are not harmonised with those set forth in the PIPA, including Art 63 relating to international data transfers. Art 63 of the Network Act will remain into force until it is displaced and renumbered Art39-12 in PIPA on 4 August 2020. Art 17 PIPA will remain applicable to all data controllers with the exception of ICSPs to which the specific provisions of Art39-12 will apply. Art 17 PIPA has been amended to include a new Para.4 (see below). - PIPA and the Network Act are currently enforced by MOIS and KCC respectively. PIPC will take over these roles on 4 August 2020.	consent for: i) providing data to third parties; ii) delegating processing; iii) onward transfer of data already transferred outside Korea to a third country. Where personal information is sent abroad with consent, the provider shall also take *'protective measures prescribed by Presidential Decree'* (Enforcement Decree of Network Act, Art 67). *Note*: Currently user consent is required for transferring data for outsourcing under the Network Act, whilst it is not required for outsourcing under PIPA. This distinction will be abolished when the new framework kicks in on 5 August 2020. Consent will generally not be required for outsourcing purposes under either PIPA or Network Act.			status of the recipient (local or foreign). The Enforcement Decree also provides that ICSPs must, in advance, reach an agreement on the *'protective measures'* which will be applied by the overseas recipient and reflect such agreement *'in the relevant contract'* (Art67-3). Such measures include: i) technical and administrative measures for protecting personal information; ii) measures for settling grievances and resolving disputes on the infringement of personal information; iii) other measures necessary for protecting users' personal information. Referring to these provisions, it is generally interpreted that a data exporter shall conclude a contract with the importer, as well as obtain the user's consent.		by the National Assembly.			services and for user's convenience' (and the other relevant conditions under the Network Act have been satisfied) in terms of controller-processor cross-border transfer. Art 63(2) will remain in force until 4 August 2020, until it is displaced to PIPA (new Art 39(12)). An amended version of Network Act Art 63 will be displaced to PIPA (new Art 39(12)), with the omission of the requirement that the transfer is 'necessary for the performance of the contract on the provision of information communication services and for user's convenience'. Thus, the dual test of necessity for contractual performance and user convenience for controller-processor transfers in the current version of Network Act will no longer apply to ICSPs and extended ICSPs. Under the amended PIPA (Art 17(4)), a controller will be allowed to provide personal data to another controller without the data subject's consent in conditions to be prescribed by Presidential Decree: 'within a scope that is reasonably related to the original purpose of collection' and 'after considering whether the data subject's rights would be infringed upon and/or measures to secure the integrity of the personal information have been properly taken.' However, it is too early to tell if the Enforcement Decree would remove consent requirements for overseas transfers in specific circumstances.
THAILAND **Mainly:** **Personal Data Protection Act 2019 (PDPA), s 28** Data transfers may freely take place to a foreign country or international organisation that have adequate data protection	**YES (optional)** When PDPA Chapter 3 enters into force, obtaining the data subject's consent will be one of the circumstances in which the data controller may derogate to the rule that transfers may take place only to a destination country or international organisation that has adequate data protection standards under PDPA (s 28(2)).	**CONCEIVABLE** When PDPA Chapter 3 enters into force, in the event that the data controller sends or transfers the personal data to a foreign country, unless an exemption applies, the destination country or international organisation that receives such personal data must have an *'adequate data protection standard*', and the transfer must	**CONCEIVABLE** In the event that the data controller sends or transfers the personal data to a foreign country, unless an exemption applies, the destination country or international organisation that receives such personal data must have an *'adequate data protection standard*', and the transfer must be carried out in accordance with	**YES (implicit)** When PDPA Chapter 3 enters into force, data may be transferred to a foreign country or international organisation in the absence of an adequacy decision where the receiving controller or processor provides *'suitable protection measures which enable the enforcement of the data subject's rights, including effective legal*	**YES (explicit)** When PDPA Chapter 3 enters into force, personal data may be transferred to an overseas destination in the absence of an adequacy decision where a *'Personal Data Protection Policy regarding the sending or transferring of personal data to another data controller or data processor who is a foreign country,'*	**CONCEIVABLE** When PDPA Chapter 3 enters into force, in the absence of adequacy, personal data protection policy, or other applicable exemptions, transfers will be allowed where the controller or processor provides *'suitable protection measures which enable the enforcement of the data subject's rights, including effective legal remedial measures*	**NO** Thailand is an APEC economy but as at April 2020 has not expressed an intention to join APEC CBPRs. CBPRs or PRP could eventually be among alternative solutions for data transfers in the absence of adequacy, BCRs, or another exemption, if the rules and methods as prescribed and announced by the Committee for	**CONCEIVABLE** When PDPA Chapter 3 enters into force, In the absence of adequacy, personal data protection policy, or other applicable exemptions, transfers will be allowed where the controller or processor provides *'suitable protection measures which enable the enforcement of the data subject's rights, including effective legal remedial measures*	**STATUTORY EXEMPTIONS** When PDPA Chapter 3 enters into force, transfers may take place to countries or international organisations without adequate data protection standards, if the transfer would be (s 28): (1) for compliance with the law; (…)

7 On the respective scopes of PIPA, Network Act, the concepts of ICSPs and Extended ICSPs, see Park Kwang Bae, 'Jurisdictional Report: Republic of Korea', in Regulation of Cross-Border Transfers of personal Data in Asia' (ABLI, 2018), p. 343

standards, and in accordance with the data protection rules prescribed by the Data Protection Committee. Exceptions to the 'adequacy' requirement apply in four series of circumstances: - the data subject's consent has been obtained; - specific statutory exemptions apply; - the receiving organisation provides suitable protection measures which enable the enforcement of the data subject's rights; or - the receiving organisation has put in place a *'Personal Data Protection Policy'* applicable to overseas data transfers. The Personal Data Protection Committee has the power *'to announce and establish criteria for providing protection of personal data which is sent or transferred to a foreign country or international organisation'* (s 16(5)). *Note:* The entry into force of the PDPA was scheduled for 27 May 2020. However, the date of entry into force of most chapters of the law (including s 28) has been postponed to 31 May 2021. Until then, sectoral laws may apply. Going beyond the general case, data privacy provisions exist in several other areas of law, such as sector-specific regulations or license conditions, in provisions setting out protections for certain categories of information, or in requirements specific to certain professions (e.g., as relevant to personal health information, credit bureaus, telecommunications licensees, securities companies, and financial institutions).[8]	Where consent is obtained, data subject must be informed of the inadequate data protection standards of the destination country or international organisation. The conditions for obtaining valid consent are defined in s 19 ('General provisions').	be carried out in accordance with the rules for the protection of personal data as prescribed by the Committee (s 28). The Personal Data Protection Committee has the power *'to announce and establish criteria for providing protection of personal data which is sent or transferred to a foreign country or international organisation'* (s 16(5)). It is also competent to decide on *'problems with regard to the adequacy of data protection standards'* of a destination country or international organisation (s 28, last para). The provisions of ss 15(6) and 28, combined, seem to imply that the Committee may put some jurisdictions or organisations which match the standards defined by the Committee on a 'white list', also by inference from Art 45(1) of EU GDPR after which the Act is modelled. However, this possibility would have to be clarified by the Committee when it is established.	the rules for the protection of Personal Data as prescribed by the Committee (s 28). The Personal Data Protection Committee has the power *'to announce and establish criteria for providing protection of personal data which is sent or transferred to a foreign country or international organisation'* (s 16(5)). It is also competent to decide on *'problems with regard to the adequacy of data protection standards'* of a destination country or international organisation (s 28, last para). The wording of ss 16(5) and 28, combined, do not appear to rule out the possibility that the exporting organisation may self-assess the level of protection in the country of destination, provided it follows the criteria and rules prescribed by the Committee. However, this possibility would have to be clarified by the Committee when it is established.	*remedial measures according to the rules and methods as prescribed and announced by the Committee'* (s 29(3)). Contracts could constitute *'suitable protection measures which enable the enforcement of the data subject's rights, including effective legal remedial measures'* if the rules and methods to be prescribed and announced by the Committee so allow.	and in *'the same affiliated business, or in the same group of undertakings, in order to jointly operate the business or group of undertakings.'* (ss 29(1) and 29(2)). Such policies must be *'reviewed and certified'* by the Office of the Personal Data Protection Committee.	*according to the rules and methods as prescribed and announced by the Committee'* (s 29). Certification could be among alternative solutions for data transfers which constitute such *'suitable protection measures'* if the rules and methods prescribed by the Committee so allow.	*'suitable protection measures which enable the enforcement of the data subject's rights, including effective legal remedial measures'* so allow (s 29(3)).	*according to the rules and methods as prescribed and announced by the Committee'* (s 29). Codes of conduct could be among alternative solutions for data transfers which constitute such *'suitable protection measures'* if the rules and methods prescribed by the Committee so allow.	(3) necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract; (4) for compliance with a contract between controller and other persons or legal persons for the interests of the data subject; (5) to prevent or suppress a danger to the life, body, or health of the data subject or other persons, when the data subject is incapable of giving the consent at such time; (6) necessary for carrying out the activities in relation to substantial public interest.
VIETNAM **Principle**: a common principle in the different texts that contain data protection provisions (in the absence of baseline data protection legislation) is that consent by the data subject is necessary to transfer data, irrespective of the implementation of data transfer mechanisms by the data exporter.[9] A proposal for a Draft Data Protection Decree was released on January 14, 2020 which would contain provisions on overseas data transfers. The proposal only contains an outline of the Draft Decree; the drafter (i.e., the Ministry of Public Security) is working on detailed	**YES (required)** A common principle in the different texts that currently contain data protection provisions (in the absence of baseline data protection legislation) is that consent by the data subject is necessary to transfer data, irrespective of the implementation of data transfer mechanisms by the data exporter.	**NO** None of the different texts that contain data protection provisions (in the absence of baseline data protection legislation) mention this possibility, nor is it known if the proposal for a Draft Data Protection Decree which would contain provisions on overseas data transfers would mention it.	**NO** None of the different texts that contain data protection provisions (in the absence of baseline data protection legislation) mention this possibility, nor is it known if the proposal for a Draft Data Protection Decree which would contain provisions on overseas data transfers would mention it.	**NO** None of the different texts that contain data protection provisions (in the absence of baseline data protection legislation) mention this possibility, nor is it known if the proposal for a Draft Data Protection Decree which would contain provisions on overseas data transfers would mention it.	**NO** None of the different texts that contain data protection provisions (in the absence of baseline data protection legislation) mention this possibility, nor is it known if the proposal for a Draft Data Protection Decree which would contain provisions on overseas data transfers would mention it.	**NO** None of the different texts that contain data protection provisions (in the absence of baseline data protection legislation) mention the possibility of privacy certification for data transfers, nor is it known if the proposal for a Draft Data Protection Decree which would contain provisions on overseas data transfers would mention it.	**NO** Vietnam is an APEC economy but has not joined the CBPRs, although at some point in time Vietnam would have expressed an interest in joining the APEC CPEA, as well as CBPRs.	**NO** None of the different texts that contain data protection provisions (in the absence of baseline data protection legislation) mention Codes, nor is it known if the proposal for a Draft Data Protection Decree which would contain provisions on overseas data transfers would mention them.	**NO** Under current law a data exporter cannot transfer personal information of data subjects in Vietnam to another person (in- or outside Vietnam) unless otherwise provided for by Vietnamese law or consented to by the data subject.

8 David Duncan, 'Jurisdictional Report: Thailand' in Regulation of Cross-Border Transfers of Personal Data in Asia (Asian Business Law Institute, 2018) at 388.
9 Waewpen Piemwichai, 'Jurisdictional Report: Vietnam, in Regulation of Cross-Border Transfers of personal Data in Asia' (ABLI, 2018), at 396.

content for each provision as outlined. **Cybersecurity Law (CSL) 2018, Art 26(3)** Specific online operators must store personal data in Vietnam. Art 26(3) CSL is applicable to *'domestic and foreign enterprises providing services on telecommunication networks or the internet or value-added services in cyberspace in Vietnam with activities of collecting, exploiting, analysing, and processing personal information data, data on the relationships of service users, or data generated by service users in Vietnam'*. Such enterprises must store such data in Vietnam for a specified period to be stipulated by the Government. Foreign enterprises referred to in this clause must have branches or representative offices in Vietnam. Art 26(4) further provides that the Government shall provide detailed regulations on Art 26(3). **Draft Decree implementing the requirements of CSL, Art 26(3)** *(version August 2019)* A draft Decree is expected in 2020. The latest version narrows down the scope of CSL. Domestic and foreign businesses that provide a variety of regulated services (defined in Art 26(1)(a)) must store data in Vietnam when: i) it is deemed necessary to protect national security, social order and safety, social ethics, community health (Art 26); ii) they have been notified that the service they provide is being used to commit acts of violation of Vietnamese laws but they have not undertaken measures to stop and apprehend those acts. The regulated services and types of data, the relevant authorities and the modalities of notification are specified in the draft.									