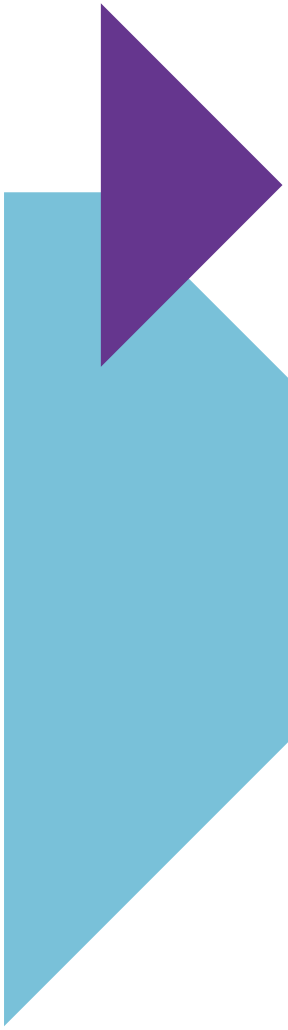
Transferring Personal Data in Asia:

A path to legal certainty and regional convergence



This Comparative Review sets out proposals for how Asian public stakeholders may promote legal certainty and greater consistency between their respective laws and regulations on cross-border transfers of personal data in the region.

Despite differences between the philosophies and the regulatory structures of each regime, there exist enough connecting points between national frameworks which lawmakers, governments, and data protection regulators can capitalize on, so as to promote and ensure responsible data flows between jurisdictions.

Interoperability would be further enhanced by a common movement to align the standards by which legal grounds, mechanisms, and schemes for data transfers should be assessed. Alignment should be with a similarly high level of data protection so as to improve the situation of individuals and facilitate multi-jurisdictional compliance, as well as regulatory cooperation.

Alignment not just to a regional standard but to global standards is a worthwhile goal, especially given the integration of Asian economies in global trade and the increased privacy expectations of the Asian public.

This Review is supported by a comprehensive comparative Table of the rules relating to the transfer of personal data in 14 Asian jurisdictions.

May 2020

ASIAN BUSINESS LAW INSTITUTE

Index

Why this Review?

Published in May 2018, ABLI's Compendium of reports on the Regulation of Cross-border Data Flows in Asia showed how, in this region as elsewhere, national data strategies generally recognise the need for rules regarding cross-border personal data transfers.[1]

In May 2020, just two years after this first publication, law reform or law review has been announced, or is under way in virtually all of the fourteen legal regimes covered in our project.

Nearly all Asian Data Protection Laws contain specific provisions applicable to cross-border data flows, and some jurisdictions are currently modifying their data protection frameworks to clarify their application to such transfers.

This trend is fuelled by the increasing relevance, in Asia, of regional or international data protection frameworks with a strong focus on international flows of personal data, including the Privacy Guidelines of the Organisation for Economic Co-operation and Development (**OECD**), the European Union's General Data Protection Regulation (**EU GDPR**), Asia-Pacific Economic Cooperation (**APEC**) Privacy Framework, Association of Southeast Asian Nations (**ASEAN**) Framework for Data Protection, and data-related clauses in trade agreements and economic partnerships, among others.

Yet, the regulation of cross-border data flows remains a key area which requires greater clarity and consistency between data privacy laws and regulations in Asia.

All the stakeholders which face the challenge of implementing these regulations, primarily industry and data protection regulators, acknowledge this necessity. Legal uncertainty and inconsistency between data protection frameworks have important repercussions on their respective actions—and, directly or indirectly, on the situation of the individuals whose personal data is transferred across the Asian borders.

ABLI wrote this Comparative Analytical Review and its supporting document—a Comparative Table on Laws, Bills, and Regulations on Personal Data Transfers in Asia, on which the Review is based—with the ambition to contribute to removing such uncertainty and unclarity in the laws of the region.

1. ABLI's Comparative Analytical Review: Promoting Convergence and Interoperability

This Review was suggested to ABLI by Asian data protection regulators and governments, who have expressed an interest in receiving comparative information to fuel their efforts to increase the compatibility or 'interoperability' of their legal and regulatory frameworks on personal data flows.

Law practitioners and industry have further expressed support to ABLI's efforts, which *'introduce an additional analytical layer to the conversation'* to which Asian Governments are currently taking part to identify common approaches to data protection between different regions.[2]

ABLI's Data Privacy Project thus features among the reasons *'why multinational organisations have good reason to hope for some measure of harmonisation of compliance standards, including practical solutions for cross-border data transfers'* in the APAC region.[3]

1 Clarisse Girot (ed), *Regulation of Cross-Border Transfers of Personal Data in Asia* (Asian Business Law Institute, 2018).

2 Derek Ho, 'Mastercard: Dealing with the complexity of data protection', *Asia Outlook*, October 2019 <https://www.asiaoutlookmag.com/industry-insights/article/775-mastercard-dealing-with-the-complexity-of-data-protection>.

3 *Hogan Lovells Asia Pacific Data Protection and Cyber Security Guide 2019* (Hogan Lovells, 2019) at 7.

The primary objective of this Review is therefore to provide lawmakers, governments, and regulators in Asia who are currently drafting, reviewing, or implementing data transfer provisions in their respective jurisdictions with a comparative overview and analysis of the transfer principles, legal grounds, mechanisms, and schemes that operate in the laws of their regional partners and neighbours.

In particular, it is hoped that the Review will be useful to those public stakeholders who are seeking constructive ways to enhance the compatibility of their respective frameworks by:

- including in Data Protection Laws or regulatory guidance the full range of available cross-border transfer mechanisms to enable accountable global data flows;
- permitting existing and widely accepted exceptions and derogations to such restrictions.

As well, it is hoped that it will help to promote the need to improve legal certainty in the application of personal data transfer restrictions, including data localisation requirements.

2. ABLI's Comparative Table on Laws, Bills, and Regulations on Data Transfers in Asia: Improving Availability and Accessibility of Asian Laws and Regulations

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.

Primary authority of non-English speaking countries might be simply lacking or be outdated as laws change rapidly and translations in other languages do not keep up. Commercial sources are expensive, and translations by government entities, when they exist, are still for informational purposes only. Only the most organised business organisations have the organisational and financial capacities to follow up on law and rulemaking and make translations to the benefit of their members.

This asymmetric level of information makes it particularly difficult for new entrants, in particular for SMEs, whether local or foreign, to assess their compliance risk. It also creates the risk that governments, lawmakers and regulators miss on feedback from lines of business that cannot afford the costs of familiarisation through local specialists. It makes it significantly harder for civil society actors like academics and NGOs to voice specific views.

This is why, in addition to this Review, ABLI has decided to publish the entire Comparative Table on Asian Laws and Regulations on Personal Data Transfers which it has drawn up to inform its analysis, for the benefit of all.

The information extracted from the Table to write this Review is current as at 28 May 2020.

The Table is published in the form of a Working Document and will be updated on ABLI's website when new laws or regulations are passed.

Key Findings

1. Collective benefits of legal certainty and convergence: Enhancing legal certainty and the compatibility of data transfer frameworks both within and between jurisdictions has a direct, collective positive impact on the respective positions of organisations, individuals, and regulators in relation to cross-border data flows.

It is an indispensable complement to any regional or international initiative intended to facilitate responsible data flows in the Asian region.

2. Major areas of differences: The mapping reveals several major areas of difference between jurisdictions:

- the rules relating to cross-border data flows can be underpinned by fundamentally different logics, which preclude looking for ambitious convergence options with some legal regimes;
- while there is overlap between legal regimes, there are differences in their regulatory structures which impact the compliance process;
- the coverage of legal grounds and mechanisms (i.e. the number available in each jurisdiction) varies; and
- implementation approaches also vary even where data transfer provisions appear consistent.

Any of these variations have great practical implications for organisations that operate in multiple jurisdictions and export data across borders.

Compliance would be greatly facilitated by ensuring maximum overlap between Asian legal systems regarding acceptable data transfer mechanisms and schemes.

3. Potential for convergence: The Review shows the potential for convergence in many transfer provisions of the Data Protection Laws, in particular for interoperability of contracts, binding corporate rules, and certification (in multiple forms) – and statutory exemptions which are recognised or could be recognised as valid in all or a large majority of Asian jurisdictions.

4. Convergence is achievable at multiple levels: Legal uncertainty, differences and inconsistencies could be removed (or at least significantly alleviated) through ongoing law reform, implementation of regulations, or issuance of *ad hoc* regulatory guidance, depending on the circumstances. Specifically, some gaps could be filled by confirmation by the regulators that specific data transfer mechanisms (e.g. certification or codes of conduct) can be read into general provisions of some laws (e.g. 'taking reasonable steps', 'comparable safeguards', or 'reasonable precautions'). Bridging such gaps would enhance the compatibility of Asian legal systems not only with each other, but also with other regional systems, primarily in Europe and the Americas.

5. Alignment on common standards: Comparisons also show that the most jurisdictions' laws remain silent on the standards by which legal grounds, mechanisms, and schemes for data transfers should be assessed (e.g. conditions for obtaining valid consent, assessment criteria for white lists, content of contracts, internal rules, operation of certification schemes, codes of conduct, etc.).

While the alignment of mechanisms is 'good enough' from the perspective of doing business, such standards should be defined consistently across jurisdictions for convergence to be truly effective.

6. Global standards: Interoperability would be further enhanced by a common movement to align these standards with a similarly high level of data protection to improve the situation of individuals and facilitate multi-jurisdictional compliance, as well as regulatory cooperation. Alignment not just to a regional standard but to global standards is a worthwhile goal, especially given the integration of Asian economies in global trade and the increased privacy expectations of the Asian public.

Ensuring consistency between global, regional and sub-regional frameworks is necessary to avoid adding more layers of complexity.

7. Guiding principles for data transfer mechanisms: Comparative analysis of Asian laws, combined with international data protection standards, leads to the conclusion that:

- any data transfer mechanism must consist in a legally binding arrangement;

- any data transfer mechanism must maintain and build upon the existing privacy protections set out in the national legislation and be consistent with principles enshrined in international frameworks and best practices;
- data subjects' rights must remain enforceable overseas; and
- adequate supervisory mechanisms must apply to the scheme or instrument to ensure effective compliance.

8. Consent: Consent appears to be an adequate legal basis for personal data transfers only in residual circumstances, and in any case not for recurrent or systematic transfers. Lawmakers should refrain from making consent compulsory in all circumstances, and provide that other solutions offering substantive protection may constitute an alternative legal basis for transfers. All solutions should be put on equal footing.

Greater coherence between the conditions in which consent-based transfers can take place in Asian legal systems should be sought. The level of details and the methods of providing consent should be addressed not in the law itself, but preferably in guidance issued of a dialogue between relevant stakeholders, which would factor in the risk of conflict between different consent requirements in the region.

9. Assessment of the level of protection in destination country: There could be some traction in developing the interoperability of data protection frameworks in the region through positive assessment findings ('adequacy'), or the recognition of the same set of substantive 'adequacy' principles adopted under multiple Asian laws. But this option requires careful consideration of the respective strengths and limitations of the 'adequacy' and 'white list' approach in Asia.

Self-assessment by the exporting organisation of the destination country's level of protection appears to be unrealistic in practice and not particularly useful to ensure the compatibility of data protection frameworks, particularly in the absence of clear criteria by which such an assessment should be made in most countries.

10. Contractual safeguards: Contracts are the most promising avenue of cooperation for increasing the compatibility of Asian data transfer regimes.

There would be traction in seeking to make the same set of contractual safeguards compatible between Asian jurisdictions, and beyond.

Convergence would be advanced if regulators would agree to a set of contractual data privacy and security controls, while allowing for flexibility in implementation. Those clauses should be detailed enough to be useful (e.g. description of envisaged transfers; applicable data protection principles; warranties, rights and obligations of the parties; complaints and compliance mechanisms; liability and enforceability by third parties; recourse of individuals; applicable law; and dispute resolution).

There is a common expectation that transfer agreements should make special provisions for the recourse of individuals whose data are transferred, although there is no uniformity on how such rights should be protected in practice.

11. Binding corporate rules: 'Binding Corporate Rules' (BCRs) are recognised as a valid data transfer mechanism in a majority of the jurisdictions covered in this Review. Until now the strengths and limitations of BCRs have been assessed only in the European context where they have originally developed, and which are partly irrelevant in an Asian context.

Leaving procedural and administrative aspects (i.e. prior authorisation by the authority) aside, the expansion of the experience on BCRs into multiple Asian jurisdictions could be explored, starting with determining whether there is a demand for this mechanism from companies operating in Asia.

12. Certification: There is a significant potential for convergence in the establishment of national certification mechanisms which would enable overseas organisations to demonstrate that they adduce acceptable safeguards to transfer data under different Asian personal data protection frameworks. This option is interesting to explore in Asia as leading personal information management certification schemes already operate in key jurisdictions like Japan or South Korea, and more recently in Singapore.

In legal regimes where certification schemes are recognised or contemplated for data transfers the laws are broad enough to allow for certification by leading international standards or schemes such as ISO/IEC 27701, or regional standards like APEC CBPRs or under EU GDPR (Art 42).

Asian governments and regulators need to work together on the certification criteria to be approved by the regulatory authority; the criteria for accreditation of certification bodies to ensure equality in independence, competence, adequate resourcing, and accountability; the identification of sufficient and clear benefits of certification to ensure organisations obtain a return on the investment to obtain certification. Regulatory focus should be on the implementation of the only schemes likely to create such motivation.

13. Cross Border Privacy Rules: The APEC Cross Border Privacy Rules (CBPRs) and the APEC Privacy Recognition for Processors (PRP) systems might benefit from a 'network effect' in Asia if more jurisdictions would join and activate either or both systems, but also if more organisations would identify benefits to certify to them.

Refining the business case of joining CBPRs would entail clarifying the interrelationship between CBPRs and the applicable local privacy laws, considering the sectors in which organisations operate, and their geographical footprint. Other factors include how the certification would help organisations earn the trust of their customers and business partners; and support the implementation of internal privacy management programmes.

14. Codes: Several Asia Pacific jurisdictions could recognise that an exporting organisation may discharge its data transfer obligations where an overseas organisation adheres to a locally approved Code of conduct or Privacy Code. This option is interesting to explore in Asia as Privacy Codes already play an important role to supplement the data protection frameworks of several jurisdictions in the region.

Such recognition would be subject to the legally binding nature of the Code and the conclusion of a contract between both the exporting and importing organisations to ensure that the safeguards of the Code (in particular, those concerning the rights of data subjects) are applied and enforced in the receiving jurisdiction.

To build coherent policies on such Codes, Asian governments and regulators need to work together on several building blocks: the criteria by which such Codes may be approved; the conditions under which Codes may be found legally binding in multiple jurisdictions; determination of appropriate recourse mechanisms for individuals in case of breach occurring overseas; criteria for accreditation of the monitoring body that will ensure compliance with the Code, to ensure equality in independence, competence, adequate resourcing, and accountability; the identification of sufficient and clear benefits of signing up to a Code to ensure that organisations obtain a return on the investment to joining that Code.

15. Exemptions: Specific legal grounds that allow personal data to flow in circumstances strictly provided by law or regulation exist in virtually all jurisdictions of this Review. Most of them take the form of statutory exemptions or derogations from the main rule applicable to data transfers (e.g., consent, adequacy).

Prima facie the different lists of national exemptions look very similar but, in effect, vary significantly so that seemingly related provisions are, in fact, difficult to compare. Ensuring greater harmonisation among exemptions will allow the same approach to be used in the same set of circumstances across several or all jurisdictions.

Whilst exceptions related to matters of sovereignty might not lend themselves to harmonisation, at least the harmonisation of more 'neutral' exceptions should be considered. Convergence efforts is to be guided by commonly agreed rules of interpretation, such as that exemptions must be interpreted 'narrowly' so that that the exception does not become the rule.

16. Administrative exemptions: In some jurisdictions organisations may solicit individual exemptions from compliance with the data transfer principles. Such exemptions are usually granted upon request, by notification, and subject to specified terms and conditions (e.g. sunset clause). Convergence could be advanced if Asian regulators would consider transposing the rationale behind such exemptions into their own frameworks, subject to similar conditions and with particular attention to the interests of individuals.

17. Data transfer mechanisms and localisation laws: Several jurisdictions currently implement, or are considering the implementation of so-called localisation measures in the Asian region. This area of the law is marked by uncertainty, particularly in jurisdictions where sweeping localisation obligations apply and where the state of the law is in constant flux.

There would be great added value in clarifying the interplay between transfer provisions in general Data Protection Laws and localisation obligations mandated in specific sectoral laws or regulations. This would include clarifying the extent of parity between 'traditional' data transfer mechanisms recognised in most jurisdictions and the conditions for approval of data transfers by the public authorities.

The scope of such localisation measures, the circumstances in which exemptions are permitted, and the regulatory expectations as to the practical consequences of mandating the localisation of some categories of data (i.e. server mirroring or other measures) should be clarified.

Entry into force periods must be of significant duration to allow organisations to take the necessary compliance measures, and extensions and adaptations should be possible on request.

Similar and consistent standards should be applied to localisation requirements in regulations applying to different sectors.

Collective Benefits of Legal Certainty & Convergence

Despite differences in cultural norms and variations in regulatory models, Asian jurisdictions share a mutual interest in bridging gaps, enhancing legal certainty and the compatibility of personal data transfer frameworks, both within and between jurisdictions.

Efforts of convergence will have a collective positive impact on the respective positions of organisations, individuals, and regulators in relation to cross-border data flows.

1. A unified set of data transfer mechanisms and schemes across multiple Asian jurisdictions would facilitate compliance with data transfer obligations by organisations to which multiple legal frameworks apply.

This would enable such organisations to choose the legal grounds, mechanisms, and schemes that are the best suited to their needs and also to rely on the same solution for each category of data transfer in each jurisdiction, avoiding unnecessary duplication of compliance efforts from one jurisdiction to the next.

Legal certainty on data transfer mechanisms would further allow organisations to streamline their accountability measures internally, but also greatly improve the time and efforts required to negotiate and enable data transfers with other organisations.

This is significantly important to SMEs and start-ups who do not have the resources and experience of dealing with complex regulation as large MNCs do. In this sense, legal certainty and convergence level the playing field.

In contrast, compliance with laws prescribing different conditions for collecting, storing or transferring data can force companies to adopt sub-optimal, hence increasingly vulnerable IT infrastructures, with significant cybersecurity risks attached.

Yet, it is not necessarily the case that data subjects' interests are demonstrably advanced by such measures through, for example, enhanced control over the use of their personal data, improved data security or regulatory oversight.

2. Removing legal uncertainty, gaps between laws, and complexity in cross-border compliance with Data Protection Laws is in the interests of individuals. Variations in scope, differences between substantive data protection rights and obligations, and between regulatory policies on data flows impede the effective cross-border implementation of individuals' data protection rights, or limit capacities for effective regulatory oversight as their data goes across borders.

As well, multiplication of compliance efforts across jurisdictions constrains organisations' internal privacy resources, which could otherwise be used to improve substantive data protection practices to benefit individuals. This includes the operational costs of planning in the face of regulatory uncertainty, adapting business, compliance functions and transactional structures to conflicting data protection or localisation requirements across different jurisdictions.

Variations in the level of protection of individuals—be they in their capacity as citizens or consumers—per country reduces public confidence and consumer trust, in both local and overseas dealings. Public stakeholders must expect that citizens will increasingly question why their national level of personal data protection might be 'lagging behind' and falling short of implementing international standards, particularly in relation to the regulation of cross-border data flows.

3. Compatible legal frameworks also help the community of Authorities to rely on other jurisdictions' learnings and approaches to implementation. Harmonisation or greater coherence between national legal frameworks, in particular in relation to the regulation of cross-border data flows, helps reduce gaps between them and thus facilitates regulatory cooperation and consistent regulatory action.

Serializing the Causes of Legal Uncertainty & Fragmentation

Seeking convergence and strengthening the consistency of legal regimes relating to cross-border data flows requires to go back to the root of their differences.

Both this Comparative Review and the Comparative Table are helpful in that they reveal the different causes of fragmentation between data transfer rules in the region. They therefore make it possible to identify the different types of policy and legal responses that can eliminate, or at least attenuate legal fragmentation and uncertainty, and consequently the different stakeholders (mainly Parliaments, governments, data protection regulators) which have the capacity to provide corresponding solutions, at their respective levels.

1. The most important factor of divergence is certainly the fact that the rules relating to cross-border data flows can be underpinned by fundamentally different logics.

Whilst most jurisdictions have adopted, or are contemplating the adoption of such rules to promote responsible data flows and avoid the circumvention or undermining of local legislative protections by transferring personal data overseas, in some jurisdictions data transfer restrictions are primarily motivated by the principle of digital sovereignty and/or by the intention to enable access by the law enforcement authorities to specific categories of personal data. In the second case, personal data must generally be kept on shore subject to governmental review, over and above obtaining the data subject's consent or implementing data transfer mechanisms like contracts, for instance.

Removing such a fundamental difference between regulations underlaid by the intention to promote free data flows on the one hand, and concerns of national security and sovereignty on the other hand, is unrealistic.

However, contact points exist even between the two types of regimes, which could anchor some actions of convergence—for instance, by clarifying the extent of parity between data transfer mechanisms in 'traditional' data protection regimes and the conditions for approval of specific personal data transfers by the public authorities (see *Data Transfer Mechanisms & Localisation Laws*→).

Such clarification would be particularly useful with regard to data transfer regimes which combine both regulatory purposes, like the Data Protection Bill of India.

2. Factors of divergence also operate between similar regimes that do not purport to significantly restrict cross-border data flows.

Most Data Protection Laws in operation in the region frame data transfers provisions as a general prohibition subject to a list of exceptions, primarily obtaining the individual's consent to the transfer ('consent-first' regimes, e.g. Japan, and South Korea) or sending data to jurisdictions with an adequate level of protection ('adequacy-first' regimes, e.g. Macau SAR, Malaysia, and Thailand). Others take the general approach that transfers should be permitted in principle but impose a requirement of 'accountability' according to which entities which transfer personal information to overseas recipients must ensure that they handle that personal information consistently with the requirements of local laws ('accountability principle') (e.g. Australia and Philippines).

3. Different default positions in the general Data Protection Law do not preclude looking for convergence options, especially when obligations relating to personal data transfers may be discharged in similar conditions.

However, the mapping done in this Review reveals three major areas of difference between jurisdictions:

First, while there is overlap between legal regimes (for example, in that the majority of regimes recognise the role of consent and contracts as permitted transfer mechanisms), **differences between the structures of data transfer regimes impact the compliance process** (e.g. whether the regime is 'consent-first', 'adequacy-first' or 'equal basis' versus 'accountability-based').

Second, **the coverage of legal grounds and mechanisms may also differ**, i.e. the number of mechanisms available in each jurisdiction is different, or it is not certain to what extent they are in overlap.

In some jurisdictions such coverage seems to be limited by intention, but it could be extended in jurisdictions that follow the same regulatory pattern depending on the decision of the regulator to take a more or less liberal interpretation of concepts such as *'transfers subject to reasonable safeguards'*, for instance.

In jurisdictions that implement the 'accountability principle' and endorse a liberal approach to data flows, ambiguity may lie in the absence of an explicit admission that some mechanisms or schemes are effective (or not) to discharge this principle.

Third, **implementation approaches also vary**, even where data transfer provisions appear consistent (e.g. subsequent guidance or subsidiary legislation may be more prescriptive on the approach to obtaining consent in one jurisdiction versus another).

As a result, it is often impossible to provide clear-cut solutions to many of the compliance issues that organisations ask themselves when navigating this area of the law in a cross-border context.

4. Any of these variations have great practical implications for organisations that operate in multiple jurisdictions and export data across borders—as multiple legal frameworks would consequently apply in cumulation, and the variance and inconsistency between jurisdictions makes the ability to apply a consistent set of compliance processes highly challenging.

This diversity in implementation is amplified by the fact that Asian legal systems have been developed at different times, under the influence of fluctuating priorities, and by reference to different regional frameworks (or to successive versions of the same frameworks).

The absence of permanent, effective pan-Asian coordination mechanisms to monitor regional developments and ensure legal consistency between different legal frameworks is another important missing element to remove fragmentation in the area of data protection and privacy.

It is hoped that this Review can contribute to advancing this regional discussion, by providing comparative information and suggestions which public stakeholders may use in their respective jurisdictions.

Paths of Convergence in a Period of Intensive Law Reform

Over the past years, a majority of Asian governments, lawmakers and regulators have worked to implement into their national legal systems high-level principles issued from frameworks such as the APEC Privacy Framework and the ASEAN Framework for Data Protection, but also principles, concepts and mechanisms found in the EU GDPR.

A complementary way of achieving the desired objective of regional consistency is to complete this high-level approach with a 'bottom-up' approach to legal convergence, by doing *'the hard and prosaic work (…) of sifting through the thicket of national laws and regulations to identify points of commonality and areas where reform is required'*.[4]

This Review and the Comparative Table contain useful information, recommendations and analyses to take this last step.

Major data protection reforms are currently happening in the region. Data Protection Bills were introduced in the Parliaments of India and Indonesia in December 2019 and January 2020, just a few months after the adoption of the new Data Protection Law of Thailand.

Law reform is underway in Australia, Hong Kong SAR, Japan, Malaysia, New Zealand, Philippines, Singapore, and was just concluded in South Korea, where implementing regulations are in a phase of public consultation.

Plans to adopt new baseline data protection regimes are made in China and Vietnam.

Localisation rules and sectoral data transfer regimes are in flux in several countries.

Delays and unpredictability in law-making, the time needed for dust to settle following such data protection reforms are further causes of legal uncertainty.

However, this time also offers a **rare window of opportunity** to dry up some sources of uncertainty and enhance the compatibility of Asian Data Protection Laws.

This Comparative Review shows how uncertainty, differences and inconsistencies can be removed (or at least significantly alleviated) through ongoing law reform, implementation of regulations, or the issuance of *ad hoc* regulatory guidance.

Specifically, some gaps could be filled by confirmation by regulators that specific data transfer mechanisms (e.g. certification and codes of conduct) can be read into general provisions of some laws (e.g. 'taking reasonable steps', 'comparable safeguards' or 'reasonable precautions').

This Comparative Review further shows that there is great potential for interoperability of some mechanisms in current laws. In particular, contracts, binding corporate rules, and certification (in multiple forms).

[4] The Honourable The Chief Justice Sundaresh Menon, *Welcome Address at Asian Business Law Institute Data Privacy Forum*, 7 February 2018 <https://abli.asia/LinkClick.aspx?fileticket=zzqdSzchQ88%3d&portalid=0>.

Analysis of Asia's Frameworks & Recommendations for Convergence

Index

Preliminary notes:

Jurisdictions covered. The jurisdictions assessed in this Review are those covered in ABLI's Data Privacy Project (see https://abli.asia/projects/data-privacy-project): Australia, China, Hong Kong SAR, India, Indonesia, Japan, Macau SAR, Malaysia, New Zealand, Philippines, Singapore, South Korea, Thailand, and Vietnam.

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 considered as part of this Review so as to avoid too wide a field of comparison.

Data localisation. Specific data transfer restrictions have been considered in jurisdictions that otherwise have, or would still have, cross-sectoral data localisation requirements (China, India, Indonesia and Vietnam), including in the two jurisdictions in this Review without a baseline Data Protection Law or Bill yet (China and Vietnam). Localisation laws are understood as measures which broadly mandate that organisations must store and/or process personal data generated within their territory, even where adequate data transfer mechanisms (e.g. contracts) have been implemented and/or the consent of the individual has been obtained.

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.

Overview of Main Rules & Principles

This section presents an overview of the baseline provisions which are applicable to personal data transfers in fourteen jurisdictions.

It shows how virtually all Asian Data Protection Laws contain specific provisions applicable to cross-border flows of personal data.

Most of them frame such provisions as a general prohibition subject to a list of exceptions, primarily obtaining the individual's consent to the transfer ('consent-first' regimes, e.g. Japan, South Korea) or sending data to jurisdictions with an 'adequate' or 'comparable' level of protection ('adequacy-first' regimes, e.g. Macau SAR, Malaysia, and Thailand).

Others take the general approach that transfers should be permitted in principle but impose a requirement of 'accountability' according to which entities which transfer personal information to overseas recipients must ensure that they handle that personal information consistently with the requirements of local laws ('accountability principle') (e.g. Australia, Philippines).

Below we consider how these main principles and rules may be discharged in each jurisdiction.

We also consider specific data transfer restrictions that take the form of cross-sectoral data localisation requirements in select jurisdictions.

Australia

Privacy Act (1988), Australian Privacy Principle (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.'*

Privacy Act 1988, s 16C: 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.

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).

China

Cybersecurity Law (CSL) 2016, NPC 12, Art 42

Informed consent of the individual is necessary to transfer or disclose any persona data to a third party (inside or outside China).

CSL, Art 37 *(in force)*

'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.

Art 37 of the 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 *(pending, latest draft version 13 June 2019)*

The draft Measures are applicable to all 'Network Operators' (not only CIIOs) and 'personal information'. 'Network operators' are *'owners and administrators of networks and network service providers'* (CSL Art 76).

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 latest draft (June 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 sensitivity levels).

Sectoral localisation obligations prevail over Art 37 of the CSL, e.g. in banking, insurance, credit reporting, health and genetics, online taxi booking and location apps. (see *Data Transfer Mechanisms & Localisation Laws* ➔)

Hong Kong SAR

Personal Data (Privacy) Ordinance (Cap. 486) 1995 (amended), s 33 *(not yet in force)*

Guidance on Personal Data Protection in Cross-border Data Transfer ('International Transfer Guidance') (December 2014)

Transfers of personal data to overseas jurisdictions are forbidden unless one of a number of conditions is met (equal basis).

These conditions include:

- 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
- 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 statutory exemptions can apply.

The International Transfer Guidance adopted by the Hong Kong Privacy Commissioner serves as a practical guide for data users to implement s 33.

Note:

Whilst s 33 PDPO is not yet in force, the Privacy Commissioner has all along been working closely with all stakeholders including the Government on its implementation.

Further to the Government's findings in its Business Impact Assessment consultancy conducted in 2016-2018, the Privacy Commissioner engaged a consultant in November 2018 to provide specialist views addressing and ameliorating the potential impact on businesses in future implementation of s 33 of the PDPO.

Amongst various recommendations, 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.

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 (IT Rule 7)

Section 43A and IT Rule 7 apply exclusively to 'sensitive personal data'.

Sensitive personal data may flow out of India when:

- the information provider has consented to the transfer; or
- 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 (IT Rule 7).

Sensitive personal data or information consists of: *'information relating to;*

(i) password;

(ii) financial information such as bank account or credit card or debit card or other payment instrument details;

(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 the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise' (IT Rule 3).

Data localisation provisions may prevail over the data transfer rules in s 43A and IT Rule 7 in specific sectors including banking, telecom, and health (see *Data Transfer Mechanisms & Localisation Laws* ➔)

India (Bill)

Data Protection Bill, 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 all transfers of personal data but only to transfers of 'sensitive' and 'critical' personal data for the purpose of processing.

Sensitive personal 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 below).

Sensitive personal data means personal data revealing, related to, or constituting, as may be applicable— (s 3(35)):

(i) passwords;

(ii) financial data;

(iii) health data;

(iv) official identifier;

(v) sex life;

(vi) sexual orientation;

(vii) biometric data;

(viii) genetic data;

(ix) transgender status;

(x) intersex status;

(xi) caste or tribe;

(xii) religious or political belief or affiliation; or

(xiii) any other category of data specified by the Authority under section 22.

Critical personal data may be processed only in India, with exceptions (s 34(2)).

Critical personal data is undefined and may be notified as such by Government regulation.

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).

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). More sectoral obligations to localise data are currently in draft, e.g. in the draft e-pharmacy rules. Localisation obligations were removed from the draft e-commerce policy in June 2019 (in anticipation of their displacement to the Data Protection Bill).

Indonesia (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

Electronic System Providers (**ESPs**) may transfer data only:

- with the individual's consent; and
- following 'coordination' with the Ministry.

The coordination requirement seems closer to a notification requirement than to a prior approval, but sometimes regulatory scrutiny is applied.[5]

[5] See Danny Kobrata, 'Jurisdictional Report: Indonesia' in *Regulation of Cross-Border Transfers of Personal Data in Asia* (Asian Business Law Institute, 2018) at 151.

Government Regulation No.71 of October 2019 (GR71), Arts 20 and 21 *(replacing Government Regulation No. 82 of 2012 (GR82))*

Specific localisation rules apply to ESPs for Public Purposes or ESPs for Private Purposes, respectively (see *Data Transfer Mechanisms & Localisation Laws*→)

Indonesia (Bill)

Data Protection Bill, Art 49 *(introduced in Parliament on 28 January 2020)*

Data transfers outside the territory of Indonesia may 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;
- international agreements apply;
- a contract offering appropriate safeguards is in place between the parties; and
- the data subject has consented to the transfer.

These provisions will be later specified in a Government Regulation.

Notes:

The Data Protection Bill will overwrite Art 26 of the EIT Law but 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 (MCI 20/2016, Art 22(1)) 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.

Japan

Act on the Protection of Personal Information, 2016 (APPI), Art 24

Transfers of personal information 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 (Art 24);
- one of a series of statutory exceptions apply (Art 23(1)).

Transfers to other 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:

- a company that enters into a merger, a company split or a business transfer with the data controller;
- data processors; or
- a company designated to jointly use the personal information with the controller.

Macau SAR

Personal Data Protection Act, 2005 (PDPA), Arts 19 and 20

The transfer of personal data to a destination outside the Macau SAR 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 (Art 19(1)).

Transfers to other destinations may take place only if specific conditions are complied with, and must be either notified to, or authorised by the Office of Personal Data Protection (Art 20):

- the data subject has given his consent unambiguously to the proposed transfer;
- the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and with respect to their exercise, particularly by means of appropriate contractual clauses;
- that transfer is necessary in varied contexts relating to the conclusion or performance of contracts, or the implementation of pre-contractual measures;
- necessary or legally required on varied statutory grounds (e.g. important public interest grounds, or for the establishment, exercise of defence of legal claims);

- necessary in order to protect the vital interests of the data subject; and
- is made from a public register.

The analysis carried out in the context of such procedures[6] appears in decisions published on the OPDP's website.[7]

Malaysia

Personal Data Protection Act 2010 (PDPA), s 129

Data transfers outside Malaysia may in principle take place only to places specified by the Minister 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 the PDPA.

Transfers to other destinations may take place only if:

- the data subject has consented to the transfer;
- reasonable precautions were taken by the data user; and
- statutory or regulatory exemptions apply.

'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).

On 14 February 2020, the Malaysian Personal Data Protection Commissioner ('Commissioner') has issued a Public Consultation Paper on the review of the PDPA.

As part of the ongoing review exercise, the Commissioner is considering issuing a guideline to address the mechanism and implementation of cross-border transfers. 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.

New Zealand (Act in force)

Privacy Act 1993, Part 11A (Transfer of Personal Information outside New Zealand), s 114B

international transfers of personal information are permitted, as long as the legal requirements in the Information Privacy Principles (**IPPs**) in Part 2 of the Privacy Act 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.

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').

6 On the operation of these procedures, see Graça Saraiva, 'Jurisdictional Report: Macau SAR' in *Regulation of Cross-Border Transfers of Personal Data in Asia* (Asian Business Law Institute, 2018) at 202.

7 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.

If data that may be legally transferred based on IPP 11 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:
    - the foreign person or entity is subject to privacy laws that, overall, provide comparable safeguards to those in the Bill;
    - the foreign person or entity is a participant in a prescribed binding scheme, or is subject to privacy laws of a prescribed country; and
    - 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 (see above).

Philippines

Data Privacy Act of 2012 (DPA) s 21

There are no specific provisions on international transfers in the DPA or its Implementing Rules and Regulations (**IRRs**).

The general rule in s 21 ('Accountability Principle') is 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 November 2019 do not modify the legal regime applicable to international transfers (but for additional transparency requirements on transfers).

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 (ss 43 and 44).

Singapore

Personal Data Protection Act 2012 (PDPA) s 26 ('Transfer Limitation Obligation' or 'TLO')

An organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA.

Personal Data Protection Regulations 2014, Part III, Regs 8-10, to be read with:

PDPC Advisory Guidelines (AG) on Key Concepts in the Personal Data Protection Act, Chapter 19

For the purposes of s 26 of the 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.

On 28 May 2020 PDPC has 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. (see *APEC Cross Border Privacy Rules*→).

PDPC Advisory Guidelines on Key Concepts in the Personal Data Protection Act, Chapter 6, paras 6.22–6.23 ('Cloud Services', revised 9 October 2019).

An organisation that engages a Cloud Service Provider (**CSP**) as a data intermediary ('processor') 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.

South Korea

Personal Information Protection Act (PIPA) Art 17 is the baseline provision on data transfers. The PIPA is complemented by **Enforcement Decree of PIPA.**

Network Act Art 63 is the specific provision relating to data transfers by Internet Content Service Providers and recipients of data collected by ICSPs (Extended ICSPs).[8] The Network Act is complemented by **Enforcement Decree of Network Act** (especially Art 67).

An overarching principle in South Korea's data protection statutes is that express user consent is required to transfer personal data to third parties whether located locally or 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:

1. 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 Art 39(12) in PIPA on 4 August 2020.

Art 17 of the PIPA will remain applicable to all data controllers with the exception of ICSPs to which the specific provisions of Art 39(12) will apply.

Art 17 of the PIPA has been amended to include a new para 4. Under this new provision, 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.

2. The PIPA and the Network Act are currently enforced by the Ministry of the Interior and Safety and the Korean Communications Commission (**KCC**), respectively.

The Personal Information Protection Commission (**PIPC**) will take over these roles on 4 August 2020. The PIPC will be responsible for the adoption of the implementing regulations of both Acts.

3. Other statutes (e.g. Credit Information Act, Location Information Act) may also apply.

Thailand

Personal Data Protection Act (27 May 2019) (PDPA) s 28 *(entry into force postponed until 31 May 2020)*

Under the new PDPA data transfers may freely take place to a foreign country or international organisation that have adequate data protection 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 (equal basis):

- the data subject's consent has been obtained;
- specific statutory exemptions apply;

[8] On the respective scopes of PIPA and Network Act, in addition to the concepts of ICSPs and Extended ICSP, see Park Kwang Bae, 'Jurisdictional Report: Republic of Korea' in *Regulation of Cross-Border Transfers of Personal Data in Asia* (Asian Business Law Institute, 2018) at 343.

- the receiving organisation provides *'suitable protection measures which enable the enforcement of the data subject's rights'*;
- the receiving organisation has put in place a 'Personal Data Protection Policy' applicable to overseas data transfers.

Note: The entry into force of the PDPA was scheduled 27 May 2020. However, the entry into force of several parts 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).[9]

Vietnam

Consent as a common principle

Currently, Vietnam does not have a baseline legislation relating to personal data flows, but various texts apply.[10]

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.

Draft Data Protection Decree

A proposal for a Draft Data Protection Decree was released on 27 December 2019 which would contain provisions on overseas data transfers.

As at 20 May 2020, the proposal still contains an outline of the Draft Data Protection Decree; the drafter (i.e., the Ministry of Public Security) is tasked with working on detailed content for each provision as outlined and is expected to release a draft 'in 2020'.[11]

Cybersecurity Law (CSL) 2018, Art 26(3)

Concurrently, Art 26(3) of the CSL impose localisation obligations on certain categories of online service providers (see *Data Transfer Mechanisms & Localisation Laws*→).

9 David Duncan, 'Jurisdictional Report: Thailand' in *Regulation of Cross-Border Transfers of Personal Data in Asia* (Asian Business Law Institute, 2018) at 388.

10 Waewpen Piemwichai, 'Jurisdictional Report: Vietnam' in *Regulation of Cross-Border Transfers of Personal Data in Asia* (Asian Business Law Institute, 2018) at 394.

11 'Proposal to develop a Decree on personal data protection', released by the MPS on the e-Government portal on 27 December 2019: <http://chinhphu.vn/portal/page/portal/chinhphu/congdan/DuThaoVanBan?_piref135_27935_135_27927_27927.mode=displayreply&_piref135_27935_135_27927_27927.id=3393>.

Consent

Obtaining an individual's consent to transfer their data is a central building block of the vast majority of data transfer regimes considered in this Review.

Consent requirements effectively play a role in relation to overseas data transfers in Australia, China, Hong Kong SAR, India, Indonesia, Japan, Macau SAR, Malaysia, Philippines, Singapore, South Korea, Thailand and Vietnam. The importance of consent requirements will be confirmed when the Data Protection Bills of India and Indonesia, and the Bill amending the Privacy Act of New Zealand are passed.

Structural differences behind apparent commonalities

However, many differences emerge behind an image of apparent unity. In fact, there are such important differences in the way 'consent' requirements work in these different settings that they effectively cancel out its potential advantages in terms of convergence actions - in any case for ongoing and systematic transfers which underlie most fundamental business processes.

Firstly, a distinction must be made according to the legal force accorded to the individual's consent and its positioning in the structure of each legal system.

Depending on the system, the individual's prior consent is:

- a systematic requisite for transferring data (irrespective of, e.g., the implementation of a transfer mechanism like a contract, or the existence of a comparable level of protection in the overseas destination);
- a requirement in principle subject to a series of exceptions (which may be more or less limited);
- one alternative among many different legal grounds for transfers; or
- irrelevant for an organisation to discharge its data transfer obligations properly.

In addition, in some systems (e.g. China and the Data Protection Bill of India), consent alone is not a sufficient ground for data transfers—at least for transfers of specific categories of data, and other conditions (e.g. approval by the public authority, implementation of additional data protection measures) apply.

Secondly, standards relating to consent also differ from country to country.

Certainly, the general conditions for valid consent overlap across jurisdictions—i.e. by and large all jurisdictions now require that consent must be 'free', 'specific' (or 'unbundled'), 'informed', and 'unambiguous'.

These qualifications interoperate with the provisions relating to the definition of consent that applies throughout the Data Protection Law, for instance for the list of situations (or legal basis) in which personal data may be legally collected and used, the circumstances in which personal information may be used or disclosed for a purpose other than the purpose it was collected for, the collection of so-called 'sensitive data' (in jurisdictions where this category is recognised), children's data, etc.

However, these general requirements may vary at implementation level. To provide only two examples:

- A common acceptation of the term 'unambiguous consent' is that consent should be express, possibly given in writing. However, in some jurisdictions (e.g. Australia and Singapore), consent can occasionally be 'deemed to be given' or 'implied' from the facts of the case, which may include failure to opt-out in some, but not all, circumstances. It is possible that a similar interpretation could be retained in relation to data transfers in other jurisdictions, but most jurisdictions have not provided such clarification.
- The concept of 'informed consent', which requires to provide different elements of information to individuals before they express their consent in relation to data transfers, also gives rise to variations in implementation.

  For example, in Australia and Thailand the exporting organisation should expressly 'inform' the individual that the same level of protection provided for under their respective domestic regimes will no longer apply after the data has been transferred overseas.

A comparable provision is to be soon adopted in New Zealand.

Singapore, on the other hand, requires that the exporting organisation must give the individual 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 Singapore law. In practice, save for specifically identified transfers to a particular organisation, it is difficult to provide such information in sufficient detail, given that each recipient will likely have implemented different ways of protecting the personal data.

Thirdly, law reform processes tend to provide that for consent to be valid, it must be freely-given, specific, informed but also 'revocable'.

This trend emphasises the need for individuals to have real choice and control over their personal data and how it is used, and consequently companies must have mechanisms and procedures in place to remove personal data from their database upon an individual's request.

Whilst there may be a willingness to accept consent as (literally) a tick box exercise in formality in some jurisdictions, the trend towards 'revocable consent' yet makes consent unworkable as a legal ground for recurring transfers in practice, unless organisations have twin servers, one onshore and one offshore, to allow data subjects to 'toggle' between where they want their data - which is not how companies are currently setting themselves up.

In such cases, obligations requiring consent for overseas data transfers may effectively require 'localisation by default' because where an individual refuses or withdraws his consent, the question naturally arises—even where such an interpretation is far removed from the lawmaker's original intention—whether the law requires servers on the ground.

Thus, it is common that practitioners advise organisations that rely on ongoing and systematic transfers of data for their operations to use another method of data transfer (in practice, the alternative written data transfer agreement route)—to the extent that other mechanisms are available.

Looking for *ad hoc* convergence actions

In this context, it is certain that any form of legal harmonisation of Asian data transfer laws around consent requirements is illusory.

This does not however preclude considering *ad hoc*, targeted convergence actions, which may allow organisations to resort to the consent solution in circumstances where consent can be given lawfully and personal data can be transferred responsibly.

The following considerations should be weighed in the balance:

- lawmakers should refrain from making consent compulsory in all circumstances and provide that other solutions may constitute an alternative legal basis (in particular, specific commitments made by organisations). For the reasons mentioned above, consent will be an adequate legal basis for data transfers only in residual circumstances, and in any case not for recurrent or systematic transfers;
- there would be real added value in seeking greater coherence between the conditions in which consent-based transfers can take place in Asian legal systems.

There is a shared concern across systems that consent requirements should not be turned into a meaningless 'tick the box' exercise with no value for individuals, in terms, for instance, of enhanced control and oversight, or facilitating the exercise of their rights, and at the same time to avoid erecting huge operational barriers for organisations.

In this respect, it is suggested that mandating in the law itself how consent is to be provided is not a viable option.

The level of details and the methods of providing consent would be better addressed in the context of a dialogue between industry and regulators which could lead to, e.g. the adoption of common findings by different national regulators on the same case studies, or in the adoption of 'Privacy Codes'. The risk of conflict between different consent requirements in the region could be factored in such a dialogue.

Status in Asia

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. It is expressed as **NO**, where obtaining the individual's consent is irrelevant in the structure of the applicable legal regime.

Australia

YES (optional)

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).

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).

China

YES (required)

Informed consent of the individual is necessary to transfer or disclose any persona data to a third party (inside or outside China) (CSL Art 41).

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).

Limited exceptions to consent for international transfers may apply, but 'security assessment' requirements will in any case remain applicable.

Hong Kong SAR

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 (PDPO, s 33(2)(b)).

Consent should be voluntarily given and not been withdrawn by the data subject in writing (International Transfer Guidance, p.5).

India (Act in force)

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 (IT Rule 7).

In any circumstances the data subject's consent is not in itself a sufficient legal ground to transfer 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 (IT Rule 7).

India (Data Protection Bill)

YES (required)

Personal data qualified as 'sensitive' under the Bill 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 (Bill, s 34(1)(a) or (b)).

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).

Indonesia (in force)

YES (required)

The written consent of the 'data owner' is required to send his/her personal data outside the territory of Indonesia, 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).

Indonesia (Bill)

YES (optional)

Transfers may take place if there is written approval from the owner of the personal data (Bill Art 49(d)). Consent can also be verbal, provided that it is recorded.

Japan

YES (optional)

Consent is required, unless exceptions apply (APPI 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).

Macau SAR

YES (optional)

Unambiguous consent to data transfer may derogate to the absence of adequate protection in destination country (PDPA Art 20(1)).

Such transfer must 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:[12]

- 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.

Malaysia

YES (optional)

Consent may operate as an exception to the requirement that transfers may take place only to places specified by the Minister (PDPA s 129(2)(a)).

New Zealand (Act in force)

NO (neither optional nor required)

Consent 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.

New Zealand (Bill)

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'* (Bill IPP12(1)(a)).

Philippines

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 of the DPA.

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.

Also, *'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) (IRRs Rule 20(b), Principles for Data Sharing).

[12] Graça Saraiva, *ibid* at 206.

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)).

Singapore

YES (optional)

The requirements of PDPA 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)).

Consent cannot be used to waive the requirement of existing privacy safeguards in the country of destination.

An individual is not taken to have consented to the transfer of the individual's personal data to a country or territory outside Singapore (PDPA Reg 9(4)) 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.

South Korea

YES (required)

Consent is required to transfer personal data to any third party, whether locally or overseas (PIPA, Art 17(1). Specific consent must be sought for transferring data overseas (PIPA, Art 17(3)).

Conditions for obtaining valid consent are prescribed in PIPA (Arts 17(2), 22).

'ICSPs' must obtain data subject's consent (Network Act, Art 63), for:

- providing data to third parties;
- delegating processing; and
- 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). The Presidential Decree has yet to be adopted.

Currently user consent is required for transferring data for outsourcing under the Network Act, but consent 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.

Art 63 of the Network Act will be displaced and renumbered to PIPA (new Art 39(12)) on 5 August 2020.

Thailand

YES (optional)

Under the recently adopted PDPA, obtaining the data subject's consent is 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 (PDPA, s 28(2)).

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 PDPA s 19 ('General provisions').

Vietnam

YES (required)

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.

'Adequacy' & 'White Lists'

Today, many data protection laws subject data transfers to the principle that 'someone' (most often a public authority, sometimes the transferring organisation) assesses the level of protection in the country of destination with regard to the processing of the imported data and finds this level of protection satisfactory for compliance with the data transfer rules applicable to the data exporter.

When a public authority issues a positive finding with regard to the level of protection of an overseas jurisdiction, the latter may be considered as providing an 'adequate', 'comparable, or 'similar' level of protection and put on a so-called 'white list', on the model of EU GDPR (Art 45).

The geographical factor also plays a role in legislations that do not follow the 'adequacy-model' but are based on the OECD Privacy Guidelines which allow data transfer restrictions where a country does not *'substantially observe the Guidelines'* or where the re-export of such data would circumvent its domestic privacy legislation, or for certain categories of personal data for which the destination country provides no 'equivalent protection'.

The geographical factor in data transfer laws and regulations in Asia

The assessment of the level of protection offered to an individual's data at its destination is a building block of the current data transfer regimes of eight jurisdictions (Australia, Hong Kong SAR, Japan, Macau SAR, Malaysia, New Zealand, Singapore, and Thailand) and of the contemplated data transfer regimes of three jurisdictions (India, Indonesia and New Zealand).

These jurisdictions generally permit transfers of personal data to countries or organisations that ensure a roughly equivalent ('comparable', 'adequate', 'substantially similar' or 'equal or higher') level of protection.

This assessment would take the form of the adoption of 'white lists' by the public authorities in the laws of four jurisdictions (Hong Kong SAR, Japan, Macau SAR, and Malaysia) and two Bills (India and New Zealand).

The Acts of Singapore and Thailand provide that the public authorities could set out the criteria for assessing the level of protection in foreign jurisdictions in guidelines or *ad hoc* regulations but do not literally provide for the adoption of white lists (such would be the intention in Thailand, but in any case, not in Singapore).

The possibility of adopting a white list seems uncertain in the current wording of the Bill of Indonesia but should be clarified in a future regulation.

Malaysia's PDPA currently allows for putting countries on white lists but to date has not adopted such lists. An announcement was made after a Consultation Paper sought feedback from the public on a draft white list of countries to which personal data originating in Malaysia may be freely transferred.[13] To-date the while list has not been issued. and Malaysia is considering removing this possibility in future amendments to the PDPA.

Recent developments in Asia

Recent developments indicate that there could be some traction in developing the interoperability of data protection frameworks in the region through positive assessment findings, or at least through the recognition of the same set of (substantive) principles adopted under multiple Asian laws. For instance:

[13] Public Consultation Paper No. 1/2017, 'Personal Data Protection (Transfer of Personal Data to Places outside Malaysia) Order 2017'.

- On January 23, 2019, the Personal Information Protection Commission of Japan[14] and the European Commission[15] announced the adoption of mutual adequacy decisions, thereby creating the first mutual system for data flows that allows businesses to send personal data back and forth between the EEA and Japan without the need to implement additional data transfer mechanisms.
- Similar negotiations have been held between the EU and the Republic of Korea since 2015.
- Following the adoption of the EU-Japan adequacy decision, the Dubai International Financial Centre (DIFC) has placed Japan on its own white list (although the 'supplementary rules' negotiated to apply to EU data transferred in Japan do not extend to Dubai residents).[16]
- New Zealand (which obtained EU adequacy status in December 2012) is updating its Privacy Act in order to ensure that it continues to meet that adequacy standard. The law reform process includes the reinforcement of the Privacy Commissioner's powers with regard to data transfers and contemplates *'prescribing countries and/or binding schemes'* as providing comparable safeguards to those in the Act (IPP 12).[17]
- In India, the White Paper released by the Justice BN Srikrishna Committee on 27 November 2017 generally opined that the adequacy test is *'particularly beneficial'*, and the proposed Data Protection Authority of India should therefore be able to determine it to ensure *'a smooth two-way flow of information critical to a digital economy'.* There would further be a great degree of geopolitical and economic interest from both EU and India in granting the latter an adequacy status *'that would benefit investment, trade and security cooperation'*.[18]

Challenges of the 'adequacy-model' in Asia

This option requires careful consideration of the respective strengths and limitations of the 'adequacy' and 'white list' approach in Asia.[19]

In particular, accommodating jurisdictions with different approaches to data protection and data flows in the region can be challenging.

Moreover, the capacities to commit a certain level of resource to monitor such assessments over time can be limited in some jurisdictions.

As well, the criteria by which such an assessment is to take place are only rarely specified by either the Data Protection Laws (whether passed or in draft), their implementing regulations, or guidelines issued by the data protection regulators.

To promote interoperability, convergence should not be done on the lowest common denominator ('any data protection law') but take account of the most developed data protection frameworks of the region.

At the same time, the most advanced adequacy criteria mentioned in EU GDPR Art 45, as interpreted by the European Court of Justice and the European Data Protection Board, are not fully transposable to an Asian context.

14 '85th Personal Information Protection Commission', *Personal Information Protection Commission,* 18 January 2019 <https://www.ppc.go.jp/aboutus/minutes/2018/20190118/> (translated) '第85回 個人情報保護委員会' 個人情報保護委員会, 平成31年1月18日.

15 'European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows', *European Union*, 23 January 2019 <http://europa.eu/rapid/press-release_IP-19-421_en.htm>.

16 "Adequate Data Protection Regimes' *Dubai International Financial Centre*, 2020 <https://www.difc.ae/business/operating/data-protection/adequate-data-protection-regimes/>.

17 Katrine Evans, 'Jurisdictional Report: New Zealand' in *Regulation of Cross-Border Transfers of Personal Data in Asia* (Asian Business Law Institute, 2018) at 253.

18 Amber Sinha and Elonnai Hickok, *ibid* at 125.

19 *Data Protection Regulations and International Data Flows: Implications for Trade and Development* (UNCTAD, 2017) at 14.

In the absence of a regional body to coordinate this creates a risk that different jurisdictions will draw contradictory conclusions regarding the same destination, which would be neither useful nor desirable with regard cross-border compliance and implementation of individuals' rights.

Such practical concerns must be factored in the assessment of the workability of such geography-based solutions in some jurisdictions.

Status in Asia

For each jurisdiction, the applicability of White Lists or Adequacy Findings for data transfers is expressed as:

- YES or NO where the legal regime either confirms or excludes 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.

Australia

NO

The OAIC does not endorse 'white lists' or 'adequacy findings' so a subjective assessment by the APP entity exporting the data is required under APP 8.1.

China

NO

Where due to business requirements it is *'truly necessary'* to provide personal information outside PRC, CIIOs shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council (unless laws or regulations provide otherwise) to conduct a cross-border transfer security assessment (CSL Art 37).

The Cyberspace Administration of China (CAC) is due to issue implementing regulations for the requirements in Art 37 of the CSL. The latest draft Cross-Border Transfer Assessment measures released by CAC (draft version 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 depending 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 version of the draft Measures).

Hong Kong SAR

YES

Data may freely flow to a place designated by the Privacy Commissioner for Personal Data (PCPD) as having a *'law substantially similar to or serving the same purpose as'* the PDPO (i.e., a 'White List Jurisdiction') (PDPO s 33(2)(a)).

Such place is specified by notice in the Gazette (s 33(3)).

India (Act in force)

UNCERTAIN

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'* the IT Rules (IT Rules, 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.

India (Bill)

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)):

- having regard to the applicable laws and international agreements; and
- 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)):

- it has previously found that the country, organisation, entity provides adequate protection; and
- 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.

Indonesia (Law in force)

UNCERTAIN

It is not known if the Ministry of Communication and Information (MCI) 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 (Arts 21 and 22).

Indonesia (Bill)

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* '(Bill, Art 49(a)).

However, the Bill does not mention which entity in the government should make that assessment, and by which criteria. Such details would be provided in future regulations.

Japan

YES

The Personal Information Protection Commission (PPC) of Japan can whitelist a foreign country establishing a *'personal information protection system'* recognised 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:

- 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 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.[20]

These standards were applied by the PPC in its decision of 18 January 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.

Macau SAR

YES

The Office of Personal Data Protection (OPDP) may decide that the legal system in the destination to which they are transferred ensures an adequate level of protection (PDPA, 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.

[20] Kaori Ishii and Fumio Shimpo, 'Jurisdictional Report: Japan' in *Regulation of Cross-Border Transfers of Personal Data in Asia* (Asian Business Law Institute, 2018) at 182.

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 (Art 19(2)).

Such transfer need not be authorised by, or notified to the OPDP.

Malaysia

YES

The 'Minister' (see below), upon the recommendation of the Commissioner, may specify any place outside Malaysia to where data may freely flow, where:

- there is in that place in force any '*law which is substantially similar to this Act, or that serves the same purposes as PDPA'*; or
- 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'* (PDPA s 129(1)).

'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).

The Commissioner is considering removal of the whitelist provisions above as part of the ongoing PDPA review exercise.

New Zealand (Act in force)

NO

The Privacy Act does not provide for the possibility to adopt white lists.

However, the Privacy 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'* set out in Part 2 of the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Privacy Act s 114B(1)(b), and Schedule 5).

There is no formal process for recognising if the receiving jurisdiction meets standards of comparability at present.

New Zealand (Privacy Bill)

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 of the Bill. The responsible Minister may recommend to the Governor-General 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'.*

Philippines

NO

Neither DPA nor IRRs refer to 'white lists' or 'adequacy findings', etc… .

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.

Singapore

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 provide to the transferred personal data a standard of protection that is at least comparable to the protection under the Act'* (PDPA s 26).

The Minister for Communications and Information could make regulations and PDPC could issue Advisory Guidelines setting out the criteria for assessment, but the PDPA does not literally provide for the adoption of white lists and such would not be the intention.

South Korea

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.

Thailand

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 the rules for the protection of personal data as prescribed by the Committee (PDPA 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'* (PDPA 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 (PDPA 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.

Vietnam

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.

Self-Assessment by the Exporting Organisation

Self-assessment by the exporting organisation of the destination country's level of protection is currently possible in Australia, Hong Kong SAR, Singapore and (under its Privacy Bill) New Zealand.

In contrast, self-assessment is excluded in Japan, Macau SAR, Malaysia and (under its Data Protection Bill) India.

Whether self-assessment is available in Thailand is not clear and still remains uncertain under Indonesia's Data Protection Bill. The uncertainty in these two jurisdictions could be clarified by implementing further regulations or regulatory guidance.

Law practitioners have expressed the view that individually assessing the 'adequacy' of every other country's privacy regime creates a substantial practical burden, especially when the law does not list substantive standards to establish that the law of another jurisdiction offers a substantially similar level of data protection.[21]

Industry groups have also argued that such assessment is unrealistic and risks becoming immediately obsolete due to changing circumstances on the ground and that, if such a task were achievable and the necessary expertise and language skills available, the theoretical legal 'adequacy' of a particular regime does not address issues such as actual compliance, enforcement or enforceability in the evaluated jurisdictions.[22]

For the purpose of achieving legal convergence in Asia, self-assessment by the exporting organisation itself is not particularly useful as it does not ensure the compatibility of data protection frameworks—or then only superficially.

Even where self-assessment is recognised as a valid option for cross-border data transfers, clear guidance is required on how the assessment is to be done and who is qualified to do it.

Status in Asia

For each jurisdiction, the possibility for an organisation to do a self-assessment of the level of data protection in a destination country is expressed as:

- **YES** or **NO** where the legal regime either confirms or excludes 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 issued such clarification.

Australia

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)).

21 Peter Leonard, 'Jurisdictional Report: Australia' in *Regulation of Cross-Border Transfers of Personal Data in Asia* (Asian Business Law Institute, 2018) at 52.

22 *Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy: Centre for Information Policy Leadership White Paper*, 25 September 2017 at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper__final__-_essential_legislative_approaches_for_enabling_cross-border_data_transfers.pdf> at 6.

China

NO

Where due to business requirements it is *'truly necessary'* to provide personal information outside China, CIIOs shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council (unless laws or regulations provide otherwise) to conduct a cross-border transfer security assessment (Cybersecurity Law Art 37).

The CAC is due to issue implementing regulations for the requirements in Art 37 CSL. The latest draft Cross-Border Transfer Assessment measures released by CAC (draft version June 13, 2019) are applicable to all Network Operators (not only CIIOs) and personal information.

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. It is possible that such 'self-assessment' could have included an assessment of the level of protection of the country of destination.

However, 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 sensitivity levels).

Hong Kong SAR

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 (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 of the data privacy regime, the existence of equivalent provisions of the Data Protection Principles 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).

India (Act in force)

UNCERTAIN

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'* the IT Rules (IT Rules, 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.

India (Data Protection Bill)

NO

Only the Central Government can make positive assessments based on either ss 4(1)(b) or 34(2)(b) of the Bill.

Indonesia (Law in force)

UNCERTAIN

It is not known if the assessment by an 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 provided in Regulation 20/2016, Arts 21 and 22.

Indonesia (Bill)

CONCEIVABLE

The country or international organisation has *'a personal data protection level that is equal to or higher than this law'* (Bill, 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.

Japan

NO

Only the PPC can make positive assessments (i.e. put a foreign country on a white list) (APPI Art 24).

Macau SAR

NO

It is for the public authority to decide whether *'a legal system ensures an adequate level of protection'* (PDPA 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.

Malaysia

NO

Only the Minister can make related specifications (PDPA s 129(1)).

New Zealand (Law in force)

NO

The Privacy Act does not cater for this possibility.

New Zealand (Privacy Bill)

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 (IPP 12(1)(c)).

Philippines

NO

Neither the DPA nor the 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 DPA s 21.

Singapore

YES

Assessment of the standard of protection in the country or territory of destination may be done by the exporting organisation itself (PDPA, s 26).

Regarding Cloud Services, for instance, the PDPC Guidelines have 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).

South Korea

NO

Neither the current nor the amended framework currently cater for this possibility.

Thailand

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 the rules for the protection of Personal Data as prescribed by the Committee (PDPA, 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'* (PDPA, s 16(5)).

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.

Vietnam

NO

None of the different texts that contain data protection provisions (in the absence of baseline data protection legislation) mention this possibility. It is not known if the proposed Draft Data Protection Decree would contain provisions on data transfers that would mention it.

Contractual Safeguards

'Contracts' and 'data transfer agreements' which provide that the personal data will be subject to appropriate safeguards after their transfer to overseas jurisdictions are widely recognised as a valid means for an organisation to discharge their obligations under data transfer provisions globally.

Back in 2000, the OECD already noted that *'the idea of using contracts for Trans-Border Data Flows has been around for some time'*, citing the Council of Europe Model Contract (1992) later revised by the International Chamber of Commerce (**ICC**).[23]

This recognition builds on the admission that contractual provisions that address compliance with a data controller's privacy policies and practices belong to the standard safeguards that are often necessary in relationships with other data controllers, including where their responsibility is shared in a cross-border context.

Wide recognition of the validity of contracts on personal data transfer in Asia

Ten jurisdictions (Australia, Hong Kong SAR, Japan, Macau SAR, Malaysia, New Zealand, Philippines, Singapore, South Korea, and Thailand) explicitly or implicitly recognise that appropriate safeguards may be provided by 'transfer contracts' or *ad hoc* contractual provisions where processing is the purpose of data transfer.

Four other jurisdictions (China, India, Indonesia and New Zealand) are contemplating explicit legal recognition of contractual provisions for this purpose, although in different configurations.

Although there is no hard information on this point, in effect, contracts would be the most widely used transfer mechanism, in Asia and globally (even when data transfer obligations could be discharged otherwise).

There would thus be great traction in seeking to make contractual safeguards compatible between Asian jurisdictions, and beyond.

Regulatory guidance and model clauses

Substantive guidance has been issued by Asian regulators on contractual measures for cross-border data transfers, which is often a mix of recommendations for transfer for processing purposes or for other purposes.

In practice, it would appear that the different sets of EU Standard Contractual Clauses (**SCCs**) are often used as a reference, with adaptations. However, EU SCCs are sometimes considered excessive, relative to the situations in jurisdictions with no data protection legislation. Such clauses generally would then impose additional obligations and liability on data exporters in comparison to what is applicable to the data exporter by virtue of statute.[24]

This appreciation could evolve, however, as more Data Protection Laws are passed in the region. Model clauses and detailed guidance on the content of contracts are generally recognised by practitioners as useful to alleviate the significant burden involved with writing contracts (or deciding whether to accept contracts prepared by others), especially if the parties are willing to adopt model contractual clauses *verbatim* (where they are available).

For this reason, several regulators in the region have issued model contractual clauses (e.g. Hong Kong SAR) or guidelines (e.g. Australia and Singapore), which are fairly prescriptive on the protections which such contracts should contain.

Recently, the Hong Kong Privacy Commissioner has announced that it will publish an updated data transfer guidance in mid-2020 with enhanced user-friendliness and additional

[23] OECD (2000), 'Trans-border Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks', DSTI/ICCP/REG(99)15/FINAL, OECD Digital Economy Papers, No. 66, OECD Publishing, Paris at 14.

[24] David Duncan, *ibid* at 121.

guidance towards data users, especially 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 data transfer agreements.

On 11 May 2020, the Office of the Privacy Commissioner of New Zealand has announced that it is working on developing a model set of contract clauses for New Zealand agencies, on which it will publicly consult in August 2020.

It is also worth underlining that ASEAN Members are contemplating the development of *ad hoc* model clauses for data transfers as one of the components of the ASEAN Cross-border Data Flow Mechanism.

Recourse of the individual

Our comparative Review shows that there is a common expectation that transfer agreements should make special provisions for the recourse of individuals whose data are transferred.

However, there is no uniformity on how such rights should be protected in practice. Depending on the legal systems under consideration, the interests of individuals may be protected in varied ways, such as:

- an explicit requirement that data protection guarantees should be enforceable by data subjects through a third-party beneficiary clause (e.g. Hong Kong SAR, Macau SAR, Thailand and China's draft cross border transfer assessment measures);
- a right to obtain compensation for breach of the contract (e.g. Hong Kong SAR, China's draft cross border transfer assessment measures);
- a general provision that the protection of the data subject's rights should be *'effective'*, including in relation to onward transfers (data protection bill of India); and
- a requirement that data sharing agreements shall *'uphold rights of data subjects'* (Philippines).

By contrast, a right for an individual to enforce a contractual right through an ability to institute legal proceedings is unlikely to be regarded as an effective enforcement mechanism in Australia.[25]

The issues affecting the recourse of the individual under B to B contracts have been considered in detail by the OECD,[26] building in particular (but not only) on the experience of the negotiations between the EU and the International Chamber of Commerce on the EU SCCs eventually adopted in 2001, 2004 and 2010.

Transfers to 'processors'

In practice, all Asian laws require contracts for framing data transfers to (sub)processors (or 'intermediaries' or 'contractors', depending on applicable terminology), particularly for the purpose of overseas processing, outsourcing and storage (e.g. a Service Agreement or other instrument meeting the same requirements).

The relationship between the parties must be governed by a 'contract' or 'legal act' that stipulates in particular that the processor shall act only on instructions from the controller and that the obligations referred shall also be incumbent on the processor. Sub-processing is possible only with the prior agreement of the data controller.

Occasionally, there are provisions for a set of requirements that should be included in outsourcing or subcontracting agreements, including those involving data transfers, e.g. in Philippines, a global hub for the Business Processing Outsourcing (**BPO**) industry.

Cloud Service Providers (CSPs)

Guidance on transfer contracts concluded with overseas parties for processing must usually be read in complement to guidance on Outsourcing or Cloud Computing dealing in particular with issues related to the responsibility of the data exporter (for instance, issues relating to liability and indemnity, or provisions that set out how personal data is to be erased or returned to data users upon data user requests, contract completion or contract termination).

[25] 'Australian Privacy Principles Guidelines', *Office of the Australian Information Commissioner*, July 2019 at paras 8.25–8.26.

[26] OECD (2000), 'Trans-border Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks', *ibid* at 17.

Several jurisdictions (e.g. Singapore, South Korea and Hong Kong SAR) have thus published guidance (general or sectoral) in relation to contractual arrangements with CSPs and, in particular, the parties' respective responsibilities regarding data privacy and personal data transfer regulations.

A common rule is that any organisation that engages a CSP is responsible for complying with obligations in respect of any overseas data transfers in using the CSP's cloud services.

Paths of convergence

Contracts certainly are the most promising avenue of cooperation for increasing the compatibility of Asian data transfer regimes.

They are recognised as a valid transfer mechanism in all jurisdictions and in contrast with more complex, innovative schemes, their enforceability as a binding legal instrument is certain under any national framework, including in a cross-border context. Moreover, their geographical reach is not limited.

Convergence would therefore be advanced if regulators would agree to a set of contractual data privacy and security controls that organisations may implement to establish sufficient levels of protection for data leaving their jurisdictions. This could be useful in creating a greater variety of options for the transfer of data internationally—provided global, regional and sub-regional frameworks are consistent to avoid adding more layers of complexity.

Based on a comparative analysis of applicable requirements in the region, such contractual controls should contain at least the following information:

- description of envisaged transfers;
- applicable data protection principles;
- warranties, rights and obligations of the parties (including with regard to management of data breach notification procedures);
- measures to ensure that the data protection rights of individuals are implemented overseas;
- recourse of individuals, complaints and compliance mechanisms;
- liability and enforceability by third parties;
- applicable law; and
- dispute resolution.

At the same time, model contracts or standard clauses should allow for flexibility in implementation (e.g. allowing for data protection clauses to be inserted into master or multi-party agreements; allowing variation of model clauses to accommodate different industries and sectors or specific data, etc).

To strike this balance, regulators may build on various work that has been undertaken in this area including:

- the long history of contractual solutions for data transfers;[27]
- the substantive experience developed in other regions, namely in Europe (i.e., either EU SCCs approved by the European Commission, or clauses adopted by the national authorities under EU GDPR Art 46) and recommendations made by cross-border businesses on their implementation;
- the existing guidance issued by Asian regulators on such matters, for instance in Australia, Hong Kong SAR, and Singapore;
- lessons to be learnt from work ongoing on model contractual clauses at ASEAN in the context of the implementation of the ASEAN cross border data transfer mechanism;[28] and

[27] OECD (2000), 'Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks', *ibid* at 14

[28] Key Approaches for ASEAN Cross-border Data Flows Mechanism adopted at the 19th ASEAN Telecommunications and Information Technology Ministers' Meeting (TELMIN), Vientiane, October 2019.

- data protection clauses used in specific industries (e.g. Cloud computing, health, banking and finance, and BPO).

The combination of contracts with other data transfer mechanisms considered in this study, such as BCRs, codes of conduct, or certification, could also be explored.

Status in Asia

For each jurisdiction, the applicability of Contractual Safeguards 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.

Australia

YES

To discharge the Accountability Principle in 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).

Contractual measures under s 95B will generally satisfy the requirement in APP 8.1. (APP Guidelines at para. 8.18).

China

YES

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.

The draft Measures set out the terms and conditions required to be in contracts between data transferors and offshore data recipients (Arts 13–16).

The detailed obligations are broadly similar to the EU SCCs, with differences relating to compensation to data subjects and onward transfers. 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).

Hong Kong SAR

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, p.7). Since the contractual provision has been twinned with the due diligence requirement, a contract alone is usually not sufficient in practice.

In 2014 the PCPD published a set of Recommended Model Clauses for transfers outside Hong Kong which distinguish between *'core clauses'* (parties' obligations, liability and indemnity, settlement of disputes, termination) and *'additional clauses'* (on third party rights and additional obligations of the transferee).

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.

India (Act in force)

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 IT Rule 7.

India (Data Protection Bill)

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 a contract approved by the Authority'* which makes the provisions 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 would still apply (Bill, s 34(1)).

Indonesia (Law in force)

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 Art 22 of MCI 20/2016.

Indonesia (Bill pending)

YES

The transfer may take place when there is *'an agreement'* between the Personal Data Controller and a third party outside the territory of the Unitary State of the Republic of Indonesia (Bill, Art 49(c)).

Japan

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).

Macau SAR

YES

The OPDP may authorise transfers where the controller adduces *'adequate safeguards'*, *'particularly by means of appropriate contractual clauses*' (Art 20(2)).

Such transfer must be authorised by OPDP.

Malaysia

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 of contracts (PDPA s 129(2)(f)).

Contracts are further mentioned as such safeguards in sectoral Codes of conduct approved by the Commissioner.

New Zealand (Act in force)

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*.'

New Zealand (Bill pending)

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)).

Philippines

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 s 44 IRRs that specify data protection requirements for Outsourcing Agreements and contemplate both local and international data sharing.

IRRs s 20(b)(2) 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'.*

Singapore

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'* (PDPC Reg.10(1)(b)).

Any contract must (PDPC Reg.10(2); PDPC AG, Chapter 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 of PDPC AG).

Regarding the Cloud Services industry, 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'*[29] (Chapter 8 of PDPC AG ('Cloud Services')).

[29] See *In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012 and Spize Concepts Pte Ltd* [2019] SGPDPC 22 (4 July 2019) at paras. 25 and ff.

South Korea

YES

Neither the current nor the amended PIPA or Network Act 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 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'* (Art 67(3)).

Such measures include:

- technical and administrative measures for protecting personal information;
- measures for settling grievances and resolving disputes on the infringement of personal information; and
- 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.

Thailand

YES (implicit)

When PDPA Chapter 3 comes 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 remedial measures according to the rules and methods as prescribed and announced by the Committee'* (PDPA s 29(3)).

Contracts could offer *'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.

Vietnam

NO

The conclusion of contracts for transfers (locally or to overseas) is standard practice but currently not required by law.

It is not known if the proposal for a Draft Data Protection Decree would contain provisions on overseas data transfers which would mention contracts.

Binding Corporate Rules

'BCRs', 'internal rules', 'intra-group schemes, policy or safeguards for intra-group transfers' (or equivalent terminologies, hereinafter 'BCRs') are now also recognised (or could be recognised) as a valid data transfer mechanism in several Asian Data Protection Laws. There could thus be traction in seeking to make BCRs compatible between multiple Asian jurisdictions, and beyond, subject to an expression of business interest.

BCRs have been developed in the EU as a cross-border transfer mechanism consistent with the transfer requirements in Directive 95/46/EC (Art 25), now in EU GDPR (Art 47).

They are data protection policies adhered to by companies for transfers of personal data within a group of undertakings or enterprises. Their key elements are fairly standardised under EU law. Similar to a code of conduct, they ensure compliance with local law, as well as adequate protection for data transferred across borders. They establish uniform internal rules for transferring personal data across the corporate group and are binding on all relevant entities and personnel in the group.

They also require a comprehensive privacy program and compliance infrastructure, including governance mechanisms, data protection officers (**DPOs**), policies and procedures, training and communication, audits and assessments and, in general, follow the essential elements of accountability and corporate compliance programs.

Under EU law there exist two types of BCRs:

- 'BCR-Controllers' (**BCR-C**) are suitable for framing transfers of personal data from Controllers subject to transfer restrictions to other Controllers or to Processors (established overseas) within the same group; and
- 'BCR-Processors' (**BCR-P**) apply to data received from a Controller subject to data transfer restrictions which is not a member of the group and then processed by the concerned group members as Processors and/or Sub-processors.

Transfers may take place on the basis of BCRs within a group of undertakings, or '*group of enterprises engaged in a joint economic activity*' (EU GDPR Art 4(20)).

BCRs are required to be approved by the data protection authority (DPA) in each EU Member State in which the organisation will rely on the BCRs, in accordance with the so-called consistency mechanism if the approval process involves DPAs from more than one Member State (Art 63). To that extent, they are a form of certification

Given the cost of implementing BCRs (both in terms of finance and resourcing) in comparison with using e.g. model contracts, BCRs are beneficial for companies that do so many complex transfers globally that they become cost-effective. For the same reason, they are usually considered maladapted to SMEs. In the long run, experience would show that—at least in an EU context—compliance costs will generally be less than the cost of other ways of handling complex intra-group transfers.[30]

BCRs and internal rules in Asian laws

Several Asian Data Protection Laws allow cross-border transfers based on 'internal rules' or 'binding corporate rules' that provide for uniform and high-level protection and privacy compliance by all local entities of a multinational group, among other data transfer mechanisms and schemes.

Such rules are explicitly recognised as a valid data transfer mechanism in the laws of, or regulatory guidance issued in six jurisdictions (Australia, Hong Kong SAR, Japan, New Zealand, Singapore, and Thailand) and in India's Data Protection Bill.

BCRs could further be read in the laws of Macau SAR, Malaysia and Philippines, as well as the Data Protection Bills of Indonesia and New Zealand.

[30] *Data Protection and Privacy 2019* (Allen & Overy, 2019) <https://www.allenovery.com/global/-/media/allenovery/2_documents/practices/corporate_and_m_and_a/data_protection/data_protection_and_privacy_november_2019.pdf> at 6.

Unique among our Review (but somehow consistent with the European experience), Thailand's PDPA and India's Data Protection Bill require that any such rules are approved by the public authority prior to implementation.

However, no particular clarification has been provided in any of these jurisdictions on whether different types of BCRs (i.e., BCR-C or BCR-P) would be acceptable, or if transfers may take place on the basis of BCRs only within a group of undertakings, or within a larger group of enterprises engaged in a joint economic activity on the model of EU GDPR Art 4(20).

Exploring the potential of BCRs in Asian laws

Up until now, Asian regulators have tended to steer away from promoting the use of binding corporate rules. In fact, the strengths and limitations of BCRs have been assessed only in the European context where they have originally developed, and which are often irrelevant in an Asian context.[31] Rather than an opposition to such a solution in principle, however, it would seem that the lack of interest can be attributed to the perception that BCRS are an 'EU solution' that cannot be readily transposed into Asia, in particular because of the administrative requirements applicable under the EU cooperation procedure.

Leaving the administrative aspects aside, the expansion of BCRs into Asia could be explored, starting with determining whether there is a demand for this mechanism from companies operating in Asia (irrespective of whether they have already put such rules in place for personal data transfers from their EU entities).

Status in Asia

For each jurisdiction, the applicability of Binding Corporate Rules 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 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.

Australia

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)

China

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 refers to *'the contracts or other legally binding measures ('the Contracts')'*. One could argue that BCRs, if they are effectively *'binding'* under Chinese law and contain the required elements in the draft measures, could be a positive factor for the purpose of the security assessment by CAC.

[31] Because BCRs have to be approved by EU Data Protection Authorities, the process can take a long time (one year in average), due to the process of coordinating several, if not all EU DPAs within the same procedure.

Hong Kong SAR

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 of the PDPO (cf. PDPO s 33(2)(f) and PCPD's International Transfer Guidance at 7).

India (Act in force)

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 IT Rule 7.

India (Data Protection Bill)

YES

Sensitive personal 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:

- effective protection of data principal's rights, including in relation to onward transfers; and
- liability of the data fiduciary for harm caused due to non-compliance.

Consent requirements still apply (s 34(1)).

This provision applies to 'sensitive personal data' (Bill s 34(1)(a)) but does not apply to 'critical personal data', nor to data that is neither sensitive nor critical under the Bill.

Indonesia (Law in force)

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'* (MCI 20/2016, Art 22).

Indonesia (Bill pending)

CONCEIVABLE

It is not certain that BCRs would be covered by Art 49(b) providing that transfers can take place when there is *'an agreement'* between the controller and an overseas third party, for instance when an intra-group agreement would support the BCRs. Such clarification would need to be made by further implementing regulations or guidance.

Japan

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'* (APPI Art 24).

Macau SAR

CONCEIVABLE

It is uncertain, but conceivable 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 Art 20 PDPA.

Such transfer would have to be authorised by OPDP.

Malaysia

CONCEIVABLE

It is uncertain, but conceivable that the Commissioner would recognise BCRs and internal rules as *'reasonable precautions'* and measures of *'due diligence'* in the meaning of s 129(2)(f) of the PDPA.

New Zealand (Act in force)

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.'*

New Zealand (Privacy Bill)

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'* (Bill, IPP12(1)(f)).

BCRs would likely qualify as such *'comparable safeguards'* as an extension of current regulatory guidance (see above).

Philippines

CONCEIVABLE

It is conceivable that the implementation of BCRs can discharge the responsibility of an organisation under s 21 of DPA for exporting '*personal information originally under its custody or its control*', including for processing.

It is also conceivable that BCRs for processors could qualify as *'reasonable means'* under s 21(a) of DPA 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'*.

Singapore

YES

'Legally enforceable obligations' that provide a level of protection comparable to PDPA in the meaning of S26 include obligations that can be imposed on the recipient by 'binding corporate rules', which may be adopted in '*instances where a recipient is an organisation related to the transferring organisation and is not already subject to other legally enforceable obligations in relation to the transfer'* (PDPC Reg 9).

BCRs must (PDPC Reg10(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 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 related to the transferring organisation if (Reg 13(3)(d)):

- the recipient, directly or indirectly, controls the transferring organisation;
- the recipient is, directly or indirectly, controlled by the transferring organisation; or
- the recipient and the transferring organisation are, directly or indirectly, under the control of a common person.

South Korea

NO

Neither the currently applicable nor the amended framework refer to BCRs.

Thailand

YES (explicit)

When PDPA Chapter 3 comes 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,'* and in *'the same affiliated business, or in the same group of undertakings, in order to jointly operate the business or group of undertakings*' (PDPA, S29(1) and (2)).

Such policies must be *'reviewed and certified'* by the Office of the Personal Data Protection Committee.

Vietnam

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.

Certification

Voluntary data protection certification mechanisms, data protection seals and privacy trust marks are set to play an important role in modern accountability frameworks for data protection and they offer promising perspectives for interoperability, in Asia and globally.

In recent years an increasing number of jurisdictions (Japan and South Korea among pioneers) have worked towards establishing certification schemes, to help organisations demonstrate compliance with local data protection regulations.

In practice, the concepts of certification, seals and trust-marks are equivalent (although different elements of the certification process can be separated and performed by different actors). They are all party attestation of conformity to a defined set of norms by third-party certification bodies that are held accountable by independent authorities to assure competence and impartiality.

Broadly speaking there are three potential advantages to organisations who obtain privacy certifications:

- it is a way of demonstrating compliance with the national Data Protection Law to businesses, individuals and regulators, in a practical way ('accountability');
- it would be a competitive business advantage and 'buying factor' when it comes to choosing vendors in their supply chain;[32] and
- eventually, under circumstances to be defined per legal regime, certification by an organisation to a national scheme in an overseas jurisdiction would enable that organisation to discharge the data transfer obligations to which it is subject when it seeks to transfer personal data from that jurisdiction.

Certification for data transfers in Asian laws

In fact, today few jurisdictions have effectively taken the necessary steps to bring about this second advantage, in Asia or globally.

However, this Review reveals a significant potential for convergence in the establishment of national certification mechanisms for overseas organisations to demonstrate that they adduce *'reasonable precautions', 'appropriate', 'adequate',* or *'comparable safeguards',* to transfer personal data under different Asian data protection frameworks.

In other words, it is possible for convergence of certification regimes to occur, so that a single organisation can be certified under multiple Asian frameworks—and potentially more—in the not too distant future.

Non-binding, self-regulatory certification mechanisms cannot *de facto* operate under the relevant data transfer provisions in several jurisdictions (e.g., Australia, Singapore, and Thailand), since it is generally necessary that certification schemes must be *'enforceable'* to be used in such circumstances.

But the admission of binding certification schemes to discharge data transfer obligations is explicit in Australia, Japan, Singapore, and in the Data Protection Bill of New Zealand. It is further implicit in Philippines and Thailand.

For now, such an admission is unclear but conceivable in the laws of Hong Kong SAR, Macau SAR, New Zealand and the Data Protection Bill of Indonesia. It is also conceivable, although more remotely, in the Data Protection Bill of India.

It was expected that reference to certification would be inserted into the data transfer provisions of the Network Act of Korea, but such reference was eventually removed from the version of the Act promulgated in January 2020.

In Asian jurisdictions where certification schemes are recognised or contemplated for data transfers the laws are broad enough to allow for certification by leading international standards or schemes such as the new standard ISO/IEC 27701:2019 on Privacy Information Management

32 'From Privacy to Profit: Achieving Positive Returns on Privacy Investments', CISCO Cybersecurity Series 2020 – Data Privacy January 2020 <https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf> at 12.

System (**PIMS**), which can potentially facilitate data flows not just from one-country-to-many-country, but data flows from most-country-to-most-country.

They could also interlace with other regional certification schemes (namely under Art 42 EU GDPR, or APEC CBPRs—see ***APEC Cross Border Privacy Rules***→), provided the level of protection provided by these schemes is aligned with national data protection requirements.

It is worth underlining that ASEAN Members are also contemplating the development of an *ad hoc* certification scheme as one of the components of the ASEAN Cross-border Data Flow Mechanism. Current plans are to articulate the ASEAN mechanism with the APEC CBPR system.

Conditions for interoperability of privacy certification schemes

For the public authorities, privacy certification mechanisms present many challenges at both conception and implementation level, starting with defining who/what can be certified (e.g. organisations, individuals, products, processes or services, or parts of those), who will deliver the certification, for how long, what certification scheme criteria must contain, and who will supervise the scheme.

At the same time, they must ensure that the schemes are relevant to the target audience, interoperable with other standards, and scalable for application to different size or type of organisations.[33]

To build coherent certification programs that may ultimately underpin legal mechanisms regulating cross-border flows in the region, it is suggested that Asian governments and regulators need to work together on three building blocks, namely:

- the certification criteria to be approved by the regulatory authority, building on the guidance and knowledge from other fields and especially technical standards to carry out the assessment of certification criteria in the data protection field;
- determination of appropriate recourse mechanisms for individuals in case of breach occurring overseas;
- the criteria for accreditation of certification bodies to ensure equality in independence, competence, adequate resourcing, and accountability; and
- the identification of sufficient and clear benefits of certification to ensure organisations obtain a return on the investment to obtain certification, and focus on the implementation of the only schemes likely to create such motivation.

Motivation for certifying to one specific scheme would be greater if that certification scheme can demonstrate accountability for many, if not all, privacy regulations, and audit once and certify for accountability in many countries simultaneously.

From a regional policy perspective, it is therefore important:

- to avoid overlap and proliferation of certifications so as to not create confusion in the minds of consumers and stakeholders, or make it less attractive for organisations seeking certification;[34] and
- to enable the alignment of such schemes not just to a sub-regional or regional standard but to global standards, in acknowledgement of the fact that relevant stakeholders (industry associations, SMEs and large enterprises) seem to favour international standards over national ones.[35]

Work is needed on all the above points to ensure that Asian certification schemes will become interoperable among one another and with other global or regional schemes.

33 Guidance of the UK Information Commissioner's Office (ICO) on GDPR Certification <https://bit.ly/2YA5dV5>.

34 CIPL Discussion Paper, 'Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms', April 2017, p. 4.

35 Irene Kamara, Ronald Leenes, Eric Lachaud, Kees Stuurman (TILT), Marc van Lieshout, Gabriela Bodea (TNO), Report to the European Commission, 'Data Protection Certification Mechanisms, Study on Articles 42 and 43 of the Regulation (EU) 2016/679' (January 2019) at 5.

Status in Asia

For each jurisdiction, the applicability of certification 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.

Australia

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). Certification could belong to such binding schemes, subject to the existence of adequate enforcement mechanisms, among other conditions.

An overseas recipient may not be subject to a 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).

China

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 other privacy seals in the region.

Hong Kong SAR

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 (p.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*'.

India (Act in force)

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 IT Rule 7.

India (Bill)

NO

The Bill does not mention the possibility for an exporting organisation to discharge the data transfer requirements in s 34 of the Bill 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 in the Bill.

Although it does not appear to be the intention, it is yet 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).

Likewise, an international or *ad hoc* bilateral agreement for certification could be concluded, which would later operate within s 34(1)(b)(i) (for sensitive personal data) or s 34(2)(b) (for critical personal data) of the Bill.

Indonesia (Law in force)

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' (MCI 20/2016, Art 22).

Indonesia (Bill)

CONCEIVABLE

Currently the Data Protection Bill does not envisage the set-up of a certification scheme in Indonesia, and it is uncertain if certification 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(b).

However, this does not rule out the possibility that an international or *ad hoc* bilateral agreement for certification could be concluded under Art 49(b) and would later operate within Art 49(c).

Japan

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 (APPI Art 24).

It has been confirmed that personal information transfers may take place under APPI Art 24 if a personal information handling business operator is certified under the CBPRs (see *APEC Cross Border Privacy Rules*→).

Macau SAR

CONCEIVABLE

It is conceivable, but not confirmed that the OPDP would take the decision to authorise a transfer based on the consideration that Certification Schemes would constitute *'adequate safeguards'* in the meaning of Art 20(2) of the PDPA.

Malaysia

CONCEIVABLE

It is conceivable, but not confirmed that certification to a privacy scheme or the obtaining of a privacy mark by an overseas organisation may constitute *'reasonable precautions'* and measures of *'due diligence'* in the meaning of s 129(2)(f) of the PDPA. Such clarification could be provided by the Commissioner.

New Zealand (Act in force)

UNCERTAIN

Regulatory guidance issued by the Privacy Commissioner 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*' under Part 11A of the Privacy Act 1993.

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.

New Zealand (Privacy Bill)

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*' (Bill, IPP12(1)(f)).

Philippines

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'* under s 21(a) of the DPA.

Likewise, it is conceivable, but not confirmed that it 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).

Singapore

YES

'Legally enforceable obligations' that provide a level of protection comparable to PDPA in the meaning of s 26 of the PDPA 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 other legally binding instrument'*.

On 28 May 2020 PDPC has amended the PDPA Regulations to recognise certification, including to the APEC CBPR and PRP Systems, as valid data transfer mechanisms under s 26 of the 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:

- The CSP based in Singapore is certified or accredited as meeting relevant industry standards; and
- 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.

South Korea

NO

Neither the current data transfer provisions in PIPA, nor Art 63 in the Network Act (to be soon transferred to PIPA and renumbered Art 39(12)) 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 by the National Assembly.

Thailand

CONCEIVABLE

When PDPA Chapter 3 comes into force, in the absence of adequacy, *'personal data protection policy'*, or other applicable exemptions, transfers are 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 according to the rules and methods as prescribed and announced by the Committee'* (DPA 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.

Vietnam

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.

APEC Cross Border Privacy Rules

The APEC Cross Border Privacy Rules system (CBPRs) and its sister system, the APEC Privacy Recognition for Processors (PRP) system, are voluntary, principles-based privacy certification mechanisms for data controllers (and in the case of the PRP, for data processors) in participating APEC member economies, based on the nine APEC Privacy Principles developed in the APEC Privacy Framework.[36]

Since APEC CBPRs is a form of certification, this section articulates with the previous section on 'Certification'.

Operation of the CBPR system

Organisations within APEC economies seeking certification under these mechanisms must have their data protection practices and procedures assessed as compliant with the program requirements by an APEC-recognised 'Accountability Agent' (**AA**) in the jurisdiction in which they have their principal place of business.

Where an APEC member economy's legislative framework either:

- does not place broad restrictions on the flow of the personal data; or
- explicitly recognises the APEC CBPR as a mechanism to transfer personal data to a recipient organisation,

then personal data from across the participating APEC membership may flow to the organisation under the certification.

Such flows are subject to oversight by the AA (which would have recourse by law or contract) and home Privacy Enforcement Authority (**PEA**) of the exporting organisation or the PEA in another participating jurisdiction (directly or through co-operation with the home jurisdiction authority).

Details on the operation of both systems are available on the dedicated CBPRs website.[37]

An important point for organisations is that CBPRs does not displace the domestic law of a participating economy. In the context of this Review, whose purpose is to promote the compatibility of national legal frameworks on personal data transfers, the key consideration is thus whether CBPR certification, whilst it cannot represent compliance with applicable local privacy laws, can still be useful to discharge at least data transfer requirements under multiple Asian Data Protection Laws.

This factor is important for businesses to assess whether the benefits of the certification outweigh its costs (human and financial costs, as well as liabilities incurred). *Cf*. the return on the investment to obtain certification (see 'Conditions for interoperability of privacy certification schemes' in ↩).

CBPR member countries—state of play

At governmental level, different situations co-exist.

To date, certification under the CBPRs for the purpose of compliance with data transfer rules has been recognised in Japan, and the scheme is also operational in Singapore following the appointment of their respective AAs. Japan Institute for Promotion of Digital Economy and Community (**JIPDEC**)—a non-profit foundation for development of key IT technologies and policies—is Japan's AA. The Infocomm Media Development Authority (**IMDA**)—a statutory board of the Singapore government—acts as Singapore's AA.[38]

36 For ease of reference the term 'CBPRs' will generally be used to cover both systems.

37 *Cross Border Privacy Rules* System, 2020 <http://cbprs.org/>.

38 Singapore has also joined the PRP system.

Certification under CBPRs has not yet been formally recognised as a means of complying with South Korea's data transfer requirements, but the scheme is now operational following the appointment of Korea Internet & Security Agency (KISA)—a suborganisation of the Ministry of Science and ICT—as South Korea's AA.

The same situation exists in Australia and the Philippines, each of whom have become members of the CBPR system in 2018 and 2019 respectively, but who are yet to appoint their respective AAs.

New Zealand is not part of the CBPR system today. However, the possibility that certification under CBPRs can satisfy impending data transfer provisions may be read into the Privacy Bill of New Zealand.

As APEC members Hong Kong SAR, Malaysia and Thailand could join the system, although to-date they have not officially expressed an interest to do so. CBPR certification for the purpose of compliance with data transfer rules is not expressly referred to (but not expressly excluded) in the current laws of Hong Kong SAR, Malaysia and Thailand.

The offices of the Privacy Commissioners of New Zealand and Hong Kong SAR (both of which are APEC members) are members of the APEC Cross-Border Privacy Enforcement Arrangement (CPEA)[39] (a pre-condition for membership in the system) and could, in principle, submit an application to join the CBPRs.

At the moment CBPR certification seems to be excluded under the laws of China and Vietnam and the Data Privacy Bill of Indonesia (all three APEC economies which could in principle join the CBPR system but have not indicated an interest in joining).

India and Macau SAR are not APEC economies and therefore cannot currently join the system.

However, APEC economies participating in the CBPR would be exploring options for expanding the reach of the CBPR given the interest among industry and other stakeholders to have a global solution for cross-border data transfers.

Options under consideration include:

- that non-APEC economies adopt similar certifications that are interoperable with the CBPR; and
- that the CBPR be globalised and opened up for participation by all qualifying countries.

Refining the business case of joining CBPRs for organisations

CBPRs (and PRP) might benefit from a 'network effect' in Asia if more jurisdictions would join and activate either or both systems, and more organisations would identify such benefits to certify to them, whether in terms of legal compliance, enhancement of privacy management programmes (PMP), and gaining shares in market competition.

As seen above, recently more Asian jurisdictions have joined the system and the system still has room for expansion.

However, until now take up of the CBPR system has been comparatively low at company level in the region. Refining the business case of joining the system would thus be worthwhile for organisations operating from this particular region.

Namely, this would entail clarifying the interrelationship between CBPRs and the applicable local privacy laws (including data transfer restrictions where they apply), considering the sectors in which of organisations operate, and their geographical footprint (and consequently the multiple laws to which those organisations are subject).

[39] The APEC CPEA aims, among other things, to provide mechanisms to promote effective cross-border cooperation between authorities in the enforcement of privacy law, including through referrals of matters and through parallel or joint investigations or enforcement actions.

This point would be all the more useful that more data protection laws are being passed in the region, which include data transfer restrictions.

Other factors unrelated to data transfers include how the certification will help organisations:

- earn the trust of their customers and business partners; and
- implement internal privacy management programmes, among others.

Status in Asia

In the list below, 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.

Australia

YES

Australia was endorsed as a participating economy in the CBPR system on 23 November 2018.

The system has not yet been implemented in Australia, and no Accountability Agent has been appointed to operate in Australia.

The Office of the Australian Information Commissioner (OAIC) will be responsible for regulating the CBPR system in Australia, once implemented.

China

NO

China is an APEC Member Economy but as at April 2020 has not indicated an intention to join CPEA or the CBPR system or PRP.

Hong Kong SAR

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 of PDPO.

India (Act in force and Bill)

NO

India is an observer to the CPEA but is currently not an APEC economy, hence the CBPRs or PRP cannot be used to demonstrate compliance with the requirements of Rule 7 under current law, or s 34 of the Bill.

Indonesia (Law in force and Bill)

NO

Indonesia is an APEC economy but as at April 2020 has not expressed an intention to join APEC CBPRs, hence certification to the CBPRs or PRP cannot be used to demonstrate compliance with the requirements under Art 21 MCI 20/2016 or Art 49 of the Bill.

Japan

YES

Japan's application to participate in CBPRs was endorsed by APEC and effective April 25, 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 Art 24. Additional requirements apply to onward transfers of data originating from the EU under CBPRs.

Macau SAR

NO

Macau SAR is not an APEC economy, hence cannot join CBPRs or PRP.

Malaysia

NO

Malaysia is an APEC economy but as at April 2020 has not expressed an intention to join the CBPR system.

New Zealand

NO

New Zealand is an APEC economy but as at April 2020 has not expressed an intention to join APEC CBPRs.

However, IPP 12 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 IPP 12(1)(d) which provides that an agency may disclose personal information to a foreign person or entity if it believes on reasonable grounds that the recipient is a participant in a 'binding scheme', i.e. *'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 s 212A by Order of the Governor-General (New Zealand's Head of State).

Philippines

YES

On 20 September 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 9 March 2020.

The system will be implemented when an Accountability Agent is appointed to operate in Philippines.

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'* under s 21(a) of the DPA.

Singapore

YES

On 20 February 2018 Singapore has joined the APEC CBPR and PRP systems, and on 17 July 2019 the Infocomm Media Development Authority (IMDA) was appointed as Singapore's Accountability Agent and three Assessment Bodies (AB) have been selected as independent bodies to assess that an organisation's data protection practices conform to the CBPR requirements.

On 28 May 2020 PDPC has amended the PDPA Regulations to recognise certification under CBPRs or PRP as compliant with s 26 of the PDPA.

South Korea

YES

The participation of South Korea in the CBPR system was approved on 12 June 2017.

The Korea Internet & Security Agency (KISA) was appointed CBPR Accountability Agent in January 2020 but certification is not yet open pending the publication of KISA's CPBR checklist.

Plans to articulate Korea's renowned Privacy Information Management System certification scheme (aka 'PIMs'), now 'Information Security Management System-Personal' (aka '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.

Thailand

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 *'suitable protection measures which enable the enforcement of the data subject's rights, including effective legal remedial measures'* under s 39(3) PDPA so allow.

Vietnam

NO

Vietnam is an APEC economy and at some point, it had expressed an interest in joining the APEC CPEA, as well as CBPRs, but to-date it has not formalised any decision to that effect.

Codes of Conduct

'Codes of Conduct', 'Codes of Practice' or 'Privacy Codes' (hereinafter, **Codes**) drawn up by industry associations and other representative bodies are very useful instruments to help organisations 'tailor-make' general data protection provisions to their specific sectors and needs.

Voluntary adherence to such codes can create market efficiencies. The association or industry body creating them conducts extensive reviews of any applicant seeking membership or otherwise desiring to claim compliance with the code. This saves an organisation, for example, from having to conduct its own assessment of a potential provider's systems, since the organisation can simply identify providers or processors who are already deemed to satisfy the requirements of the code and rely on the association to ensure compliance.[40]

Broadly speaking there are two potential advantages to the organisations that sign up to a code and the profession, industry or sector to which the code applies (which are broadly similar to those of obtaining certification):

- it is a way of demonstrating compliance with the national Data Protection Law to businesses, individuals and regulators, in a practical way ('accountability'); and
- it would be a competitive business advantage and 'buying factor' when it comes to choosing vendors in their supply chain; and
- eventually, under circumstances to be defined per legal regime, signing up to a code registered or approved and monitored in an overseas jurisdiction would enable that organisation to discharge the data transfer obligations to which it is subject when it seeks to transfer personal data from that jurisdiction.

Such recognition now exists in EU GDPR, which provide that adherence to codes, together with binding and enforceable commitments, can demonstrate that data importers located outside the EU have implemented adequate safeguards in order to permit transfers under Art 46(e) of EU GDPR.

It is therefore worth exploring if codes could effectively offer an alternative mechanism for managing international transfers to and from Asian jurisdictions.

Codes for personal data transfers in Asia

To date, none of the jurisdictions considered in this Review explicitly provide that an exporting organisation may discharge its data transfer obligations where an overseas organisation ('controller' or 'processor') adheres to a locally approved, non-binding, code.

However, some legal systems are considering recognising codes—at least on paper—as valid for such purposes, subject to:

- the legally binding nature of the code; and
- the conclusion of a contract between both the exporting and importing organisations to ensure that the safeguards of the code (in particular, those concerning the rights of data subjects) are applied and enforced in the receiving jurisdiction.

In effect, subject to conditions of enforceability, it is conceivable that compliance with a highly regulated code of practice would constitute *'reasonable precautions', 'comparable safeguards',* a *'binding scheme'* or equivalent test in Australia, Hong Kong SAR, Japan, Macau SAR, Malaysia, Philippines, Singapore, and Thailand), in addition to the Data Protection Bills of New Zealand, India and Indonesia.

Convergence would be advanced if regulators would agree to a set of conditions that such codes should implement to establish sufficient levels of protection for data leaving their jurisdictions.

40 Rita Heimes, 'Part 9: Codes of conduct and certifications' in *The Top 10 Operational Impacts of the EU's General Data Protection Regulation* (International Association of Privacy Professionals, 2016) <https://iapp.org/resources/article/top-10-operational-responses-to-the-gdpr/>.

'Privacy codes' in Asia

This option is all the more interesting to explore in Asia as privacy codes already play an important role to supplement the data protection frameworks of several jurisdictions in the region, for instance:

- In Australia, the Information Commissioner can approve and register enforceable codes which are developed by entities on their own initiative or on request from the Information Commissioner, or developed by the Information Commissioner directly. The codes are *'disallowable legislative instruments'* which do not replace the relevant provisions of the Privacy Act, but operate in addition to the requirements of the Privacy Act (Privacy Act, Part IIIB);
- In Hong Kong SAR, the Commissioner may issue and approve Codes of Practice *'for the purpose of providing practical guidance in respect of any requirements'* imposed under PDPO on 'data users' (PDPO, Part III). The Commissioner has issued several Codes of Practice, especially on Consumer Credit Data;[41]
- The Privacy Commissioner of New Zealand has issued several Codes of Practice under the Privacy Act, which have become part of the law and which modify the privacy principles in relation to specific industries.[42] The Codes will have to be updated to reflect changes under the Privacy Bill (including consideration of changes for the new IPP12 relating to the disclosure of information to overseas agencies under the Privacy Bill);
- In Malaysia, the Commissioner may either issue, or approve and issue Codes of Practice, and publish them in a Register (PDPA Art 23). Several codes have been published, for instance in the Banking and Financial Sector,[43] or in the Insurance and Takaful Industry in Malaysia.[44] The Commissioner may form and designate *'data user forums'* to the effect of preparing such codes, '*in recognition of the fact that separate sectors or industries may have specific industry practices in relation to the manner in which personal data is handled, and/or may have deployed unique technologies which require specific data protection rules.'* (Introduction, Para. 1.3 of Codes of practice adopted by the Commissioner).

Regulators may thus build on the substantive experience developed on such Codes in specific countries, as well as on:

- The guidance issued by regional regulators on such matters, such as the Guidelines for developing codes developed by the Office of the Australian Information Commissioner (OAIC) (September 2013);[45]
- Lessons to be learnt from work ongoing on Codes of Conduct under EU GDPR;[46]
- Lessons to be learnt from specific industries (e.g. cloud computing) on the conditions for uptake and the development of sectoral codes of conduct, at the national, regional, or global level.[47]

41 Code of Practice on Consumer Credit Data (2013).

42 Health Information Privacy Code (1994), Credit Reporting Privacy Code (2004), Telecommunications Information Privacy Code (2003).

43 Personal Data Protection Code of Practice for the Banking and Financial Sector (January 2017).

44 Code of Practice on Personal Data Protection for the Insurance and Takaful Industries in Malaysia (February 2017).

45 Guidelines of the Office of the Australian Information Commissioner for developing codes issued under Part IIIB of the Privacy Act 1988 (September 2013).

46 E.g., Guidelines of the European Data Protection Board 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679.

47 For instance, the code of practice developed by the cloud computing industry in New Zealand with assistance and input from the Cloud Security Alliance (CSA) and Office of the New Zealand Privacy Commissioner; or the experience of the Cloud Security Alliance on developing a Code of conduct for GDPR compliance (November 2017).

Conditions for interoperability of Codes of Conduct as data transfer mechanisms

Codes of conduct and certification are regulatory mechanisms that borrow heavily from each other, and in fact the procedural aspects of both mechanisms are also similar.[48]

The suggestions relative to the key factors that can promote the interoperability of Certification Schemes in Asia are thus partly transposable to this Section.

To build coherent policies on such codes that may ultimately underpin legal mechanisms regulating cross-border flows in several jurisdictions, it is suggested that Asian governments and regulators need to work together on several building blocks:

- the criteria by which such Codes may be approved;
- the conditions under which Codes may be found legally binding in multiple jurisdictions (since voluntary Codes are not eligible for data transfers in any jurisdiction)—e.g. through contracts;
- determination of appropriate recourse mechanisms for individuals in case of breach occurring overseas;
- the criteria for accreditation of the monitoring body that will ensure compliance with the Code, to ensure equality in independence, competence, adequate resourcing, and accountability;
- the identification of sufficient and clear benefits of signing up to a Code to ensure that organisations obtain a return on the investment to joining that Code.

Flowing from the last point, from a regional policy perspective it is important:

- to avoid overlap and proliferation of Codes so as to not create confusion among consumers and stakeholders or make it less attractive for organisations contemplating signing up;[49]
- to enable the alignment of such Codes not just to a sub-regional or regional standard but to global standards (although they must remain scalable).

Status in Asia

For each jurisdiction, the applicability of Codes of conduct under the Data Protection Law or Bill is expressed as:[50]

- NO where the legal regime is silent on the applicability of Codes;
- UNCERTAIN where the legal regime fails to address Codes 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.

Australia

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.

48 CIPL Discussion Paper, 'Codes of Conduct and Monitoring Bodies in GDPR', 29 March April 2019, p. 3.

49 CIPL Discussion Paper, 'Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms', April 2017, p. 4.

50 As noted above (see *Codes for personal data transfers in Asia*), none of the jurisdictions considered in this Review explicitly provide that an exporting organisation may discharge its data transfer obligations where an overseas organisation ('controller' or 'processor') adheres to a locally approved, non-binding, Code. Hence, no jurisdiction is marked with **YES**.

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).

China

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.

Hong Kong SAR

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).

India (Act in force)

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 IT Rule 7.

India (Data Protection 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 section 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 also uncertain (but not unconceivable) that compliance with a code registered 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).

Indonesia (Law in force)

UNCERTAIN

It is not certain if adherence of the importing organisation to a local code 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'* of Information and Communication under Art 22 of MCI 20/2016.

Indonesia (Bill)

CONCEIVABLE

It is uncertain, yet 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) of the Bill.

Japan

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 under APPI Art 24.

Macau SAR

CONCEIVABLE

It is uncertain, but conceivable that the OPDP could authorise a transfer based on the consideration that a code of conduct would constitute *'adequate safeguards'* in the meaning of PDPA Art 20(2).

Such transfer would have to be authorised by OPDP.

Malaysia

CONCEIVABLE

It is conceivable, but not confirmed by the Commissioner 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 s 129(2)(f) of the PDPA.

Section 23 of the PDPA 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.

New Zealand (Act in force)

UNCERTAIN

Neither the Privacy Act nor the Regulatory Guidance issued by the Privacy Commissioner 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.

New Zealand (Privacy Bill)

CONCEIVABLE

It is possible that voluntary adherence of the recipient to a code could contribute to an agency believing on reasonable grounds that the foreign person or entity is subject to *'comparable safeguards'* in the meaning of IPP12(1)(f) of the Bill.

Philippines

CONCEIVABLE

It is conceivable, but not confirmed under the DPA or the IRRs if adherence of a data recipient to a code 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'* under s 21 of the DPA.

Section 7(j) of the DPA provides that the NPC has the function to *'review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers*.' Section 7(j) does not make a reference to the role which such codes can play in relation to data transfers to third parties.

Singapore

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 other legally binding instrument'.* It is conceivable that codes of conduct could constitute such *'legally binding instruments'* under s 26 of the PDPA.

South Korea

NO

Neither the current nor the amended framework (PIPA or Network Act) refer to codes to discharge obligations in relation to overseas data transfers at this stage.

Thailand

CONCEIVABLE

When PDPA Chapter 3 comes into force, in the absence of adequacy, personal data protection policy, or other applicable exemptions, transfers are 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 according to the rules and methods as prescribed and announced by the Committee'* (PDPA s 29).

Codes 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.

Vietnam

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.

Exemptions & Additional Legal Grounds for Transfers

Specific legal grounds that allow data to flow in circumstances strictly provided by law or regulation exist in virtually all jurisdictions of our Review.

Many of them take the form of statutory exemptions or derogations from the main rule applicable to data transfers (e.g., consent and adequacy). The term of exemption can however be inappropriate in systems where data transfers are permissible by default subject to satisfying their respective accountability principles, since there is in place no transfer restriction to be exempted from, or to make exception to, in those jurisdictions.

Even then, the same concepts operate. For instance, data sharing shall be allowed *'when it is expressly authorised by law'* in Philippines (DPA s 21(a)), while transfers *'authorised by law or an international agreement'* cannot be prohibited by the New Zealand Privacy Commissioner (Privacy Act, s 114B(3)).

Commonalities in concepts

Transfers of personal data to overseas jurisdictions are always possible when they are necessary:

- to protect the vital interests of individuals; or
- to prevent or fight a serious threat to public health or safety.

Related provisions are found in Australia, China, Hong Kong SAR, Japan, Macau SAR, Malaysia, Singapore and Thailand), as well as the Privacy Bill of New Zealand and the Data Protection Bill of India (although, only in relation to critical personal data).

Other exemptions shared—implicitly or explicitly—by several jurisdictions apply where the transfer is:

- necessary to comply with national laws and regulations (e.g. Australia, Japan and New Zealand's Data Privacy Bill);
- required or authorised under international agreements relating to information sharing (e.g. Australia, New Zealand and Indonesia's Data Protection Bill);
- necessary for law enforcement by the national authorities (e.g. Australia, Hong Kong SAR, Japan, India's Data Protection Bill, and New Zealand's Privacy Bill);
- for the purposes of judicial activities and enforcement (e.g. Australia, Hong Kong SAR, Macau SAR, Malaysia, India's Data Protection Bill, and New Zealand's Privacy Bill); and
- national security or defence (e.g. Australia), or in the national or public interest (e.g. Macau SAR, Malaysia, Singapore, Thailand, and New Zealand's Privacy Bill).

Transfers may also be free in specific circumstances where they are necessary for the performance of a contract at the request and/or in the interest of the individual (e.g. Hong Kong SAR, Macau SAR, Malaysia, Singapore, and Thailand).

Other exemptions pertain e.g. to the transfer of de-identified data for statistics and research (Hong Kong SAR) or to the necessity of child protection (Japan), etc.

Differences behind apparent commonalities

Prima facie the different lists of national exemptions look very similar but, in effect, vary significantly so that seemingly related provisions are, in fact, difficult to compare.

As mentioned earlier, exemptions may apply to different rules and principles for transfers in each jurisdiction. For example, the exemptions may apply to the consent requirements under South Korea's law, to the existence of an adequate level of protection overseas under Thai law, or to the 'accountability principle' under Australian law (*cf.* *'Serializing the Causes of Legal Uncertainty & Fragmentation'*↩).

Some exemptions are common to most local Data Protection Laws, but not all of them are in complete overlap, and some concepts (e.g. public interest, necessary for law enforcement) could be interpreted differently. The 'research' exemption applicable to de-identified data in Hong Kong PDPO and India's Bill, the necessity of child protection in Japan or the localisation of a missing person in Australia, for instance, have no direct equivalent in other jurisdictions, although the regulators and the courts might accept to read the same concepts into wider exemptions.

It is not only exemptions from the data transfer requirements that must be considered. The transfer restrictions may apply to all types of personal data, or to specific types of data only (e.g., sensitive or critical personal data in India).

As well, restrictions on the general scope of the laws necessarily flow through to exemptions from data transfer requirements.[51] These 'upstream' exemptions also vary among the jurisdictions of this Review (see, for example, exceptions for 'publicly available information' in Singapore and Australia; exclusion of 'non-commercial' activities in Malaysia).

Sometimes, different standards apply to data processed overseas or originating from overseas (e.g., New Zealand, Philippines, Data Protection Bill of India).

Ensuring greater harmonisation among exemptions will allow the same approach to be used in the same set of circumstances across several or all jurisdictions.

Whilst exceptions related to matters of sovereignty (e.g. national or public interest, national security or defence) might not lend themselves to harmonisation, at least the harmonisation of more 'neutral' exceptions (e.g. performance of a contract and vital interests, etc.) should be considered.

The current Covid-19 crisis certainly provides the right conditions to collectively test the contours of exemptions relating to public health and safety, protection of the vital interests of individuals, and research.

Common rules of interpretation

Convergence efforts could be guided by the commonly agreed rules of interpretation that:

- exemptions must be interpreted *'narrowly'* (i.e., Hong Kong SAR) or applied in *'exceptional'* circumstances (i.e., Japan);
- exemptions are subject to a test of *'reasonableness'* or where it is not *'reasonably practicable'* (see, for instance, the tests in Australia, Hong Kong SAR and New Zealand's Privacy Bill); and
- appropriate safeguards for data privacy and security must be provided where transfers are allowed under national laws and regulations or international agreements (e.g. Philippines) so as to preserve the consistency of the wider data protection framework.

Exemptions from data transfer rules by the Authority

Finally, in some jurisdictions (e.g. Malaysia, Singapore and India's Data Protection Bill) the data protection regulators or the government may exempt organisations from compliance with specific provisions of the Data Protection Law, sometimes including the data transfer principles. Such exemptions are usually made upon request, by notification, and subject to specified terms and conditions.

Exemptions may be granted on an individual or collective basis (e.g. 'class of users' in Malaysia).

The scope of exemptions granted by the authorities varies, however.

Some of them are broad and may cover any provision in the Data Protection Law. Others are more targeted and relate only to specific purposes, and/or to specific categories of data. For instance, exemptions from any provisions in the Data Protection Bill of India are possible when the Authority is satisfied that the processing is necessary for 'research, archiving or statistical purposes', under specific conditions including de-identification and absent any risk of significant harm to the individual (Bill s 38).

51 UNCTAD report, 'Data protection regulations and international data flows', *ibid* at 8.

Comparisons also reveal that the standards applicable to administrative exemptions from the applicability of data transfer provisions do not overlap.

For instance, in September 2017 Singapore's Personal Data Protection Commission announced that it would create regulatory sandboxes on the basis of s 26(2) PDPA to exempt organisations from the transfer limitation obligation, subject to specific criteria. An exemption 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 must provide exceptional and compelling reason(s), accompanied with evidence of the reason(s) why the organisation is unable to comply with– in this particular case– s 26 of the DPA.

In contrast, in India some provisions might be excluded, but the data transfer restrictions would in any case remain applicable to any organisation participating in the regulatory sandbox to be created by the Data Protection Authority of India (Bill s 40).

Convergence could be advanced if Asian regulators would consider transposing the rationale behind such exemptions into their own frameworks, subject to similar terms and conditions.

This possibility could be envisaged in particular for exemptions relating to categories of organisations.

This pre-supposes that the motives of decisions to exempt organisations from specific obligations or principles would be made public to enable comparisons between jurisdictions' approaches to implementation.

As well, it would be appropriate to provide explicitly that key obligations (e.g., transparency, security, performance of data protection impact assessments– in particular when sensitive data is concerned, fair and reasonable processing) still are to be complied with.

Status in Asia

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.

Australia

STATUTORY EXEMPTION

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' (Privacy Act s 16A) exists in relation to the disclosure of the information by the entity, which is necessary to:
  - lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety;
  - in relation to suspected unlawful activity or serious misconduct;
  - locate a person reported as missing;
  - for a diplomatic or consular function or activity; and
  - for certain Defence Force activities outside Australia.

China

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.).

However, this provision is only in relation to domestic transfers. Neither the Personal Information Security Specification nor the current version of the Draft Cross-Border Transfer Assessment measures mention if any overseas data transfers may be exempted from this assessment procedure, or from the consent or contract requirements.

Hong Kong SAR

STATUTORY EXEMPTIONS

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 (PDPO s 33(2)(e)).

The transfer may also take place when the user has reasonable grounds for believing that, in all the circumstances of the case (PDPO 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 p.6).

India (Act in force)

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.

India (Data Protection Bill)

STATUTORY EXEMPTIONS

Varied exemptions to the data transfer provisions (Chapter VII) are provided in Chapter VIII of the Bill ('Exemptions').

With regard to statutory exemptions, s 36 (a) to (d) provide that in particular the data transfer restrictions in Chapter VII of the Bill will not apply when data transfer of any personal data is necessary for the purposes of—

- law enforcement;
- legal proceedings;
- exercise of any judicial function;
- domestic purposes; or
- journalistic purposes.

Further, critical personal data may 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 AUTHORITY

Organisations may be exempted by the DPAI from the application of any provision of the Bill (including Chapter VII on data transfer restrictions) for the purposes of research, archiving, or statistical purposes, irrespective of

the nature of the personal data, provided specific conditions are complied with.

The DPAI may, by notification, exempt such class of research, archiving, or statistical purposes from the application of any of the provisions of this Act, as may be specified by regulations (s 38). It 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.

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.

Indonesia (Law in force)

NO

Currently no exception to consent or additional legal ground apply for transfers outside the territory of Indonesia.

Indonesia (Bill)

ADDITIONAL LEGAL GROUND

Transfers may take place when *'there are international agreements between the countries'* (Art 49(b)). However, the Bill does not clarify the nature or the content of the agreements which would be covered by this provision.

Japan

STATUTORY EXEMPTIONS

Transfers may take place without the user's consent in the following circumstances (APPI 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 performance of the said affairs.

Macau SAR

STATUTORY EXEMPTIONS

A transfer of personal data to a destination in which the legal system does not ensure an adequate level of protection may be allowed where the transfer (PDPA Art 20(1)):

(1) 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) 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) *is necessary or legally required on important public interest grounds, or for the establishment, exercise of defence of legal claims;*

(4) *is necessary in order to protect the vital interests of the data subject;*

(5) *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 in any case be notified to OPDP.

Malaysia

STATUTORY EXEMPTIONS

Transfers of personal data may take place to other non-adequate destinations if (PDPA s 129(3)(b)–(h)):

(a) *[...]*
(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*
(f) *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.*

EXEMPTION BY THE AUTHORITY

A data user or class of users may be exempted from all or part of the PDPA (including PDPA s 129) by decision of the Minister following the prior opinion of the Commissioner (PDPA s 46(1)).

New Zealand (Act in force)

STATUTORY EXEMPTIONS

The Commissioner may not prohibit a transfer if it is (Privacy Act 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)

New Zealand (Privacy Bill)

STATUTORY EXEMPTIONS

No restriction applies to overseas data transfers:

- if it is '*not reasonably practicable in the circumstances'* to comply with the requirements of IPP 12(1) (IPP 12(2)); *and*
- the disclosure of the information *is necessary* (IPP 10(1)(e)):
  - (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*
- the disclosure of the information *is necessary to prevent or lessen a serious threat to* (IPP 10(1)(f)):
  - (i) *public health or public safety; or*
  - (ii) *the life or health of the individual concerned or another individual.*

Moreover, the same policy as in Privacy Act s 114B(3) (see 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

ADDITIONAL LEGAL GROUND

No exception is provided to the accountability principle in s 21 of the DPA.

However, s 20(a) of the 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

STATUTORY EXEMPTIONS

Transfers of personal data would be allowed 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 when:

- the transfer of personal data 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 of personal data 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 (Reg 9(3)(d));
- the personal data is data in transit (Reg 9(3)(f));
- the personal 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 (PDPA s 26(2)).

In September 2017 the PDPC announced that it would create 'regulatory sandboxes' on the basis of this Section to exempt organisations from the transfer limitation obligation, and subject to specific criteria.

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—in this particular case—PDPA s 26.

South Korea

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 Art 63(2) of the Network Act consent is not required where the delegation by the ICSP is '*necessary for the performance of the contract on*

the provision of information communication 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 Art 63 of the Network Act will be displaced to PIPA as a 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

STATUTORY EXEMPTIONS

Under the new PDPA transfers may take place to countries or international organisations without adequate data protection standards, if the transfer is (PDPA s 28):

(1) for compliance with the law;

(2) […]

(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

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.

At this stage it is not known if the proposal for a Draft Data Protection Decree which would contain provisions on overseas data transfers would provide for exemptions similar to those in place in other jurisdictions.

Data Transfer Mechanisms & Localisation Laws

Several Asian jurisdictions have implemented or are considering implementing so-called 'data localisation' measures. These measures broadly mandate that organisations must store and/or process personal data generated within their territory, even where specific data transfer mechanisms (e.g., contracts) have been implemented and/or the consent of the individual has been obtained by the organisation. Data exports may take place in derogation to such localisation measures only in specific circumstances, and normally after approval by a public authority.

Since localisation provisions increasingly appeal to the principle of digital sovereignty or purport to enable access by law enforcement to specific categories of personal data, other factors than the protection of privacy weigh in the assessment done by the public authority.

The policies underlying these requirements, their implications, and the arguments of stakeholders arguing both for or against them, have been exposed in detail elsewhere.[52]

Such measures can be contrasted with 'traditional' data transfer provisions found in Data Protection Laws, which are not effectively designed to keep data on shore but to avoid circumvention or undermining of local legislative protections through overseas personal data transfers.[53] Such obligations can be discharged by organisations without *ex ante* oversight of each transfer by the authority, e.g. by implementing one of the mechanisms considered in this Review (contracts, BCRs, etc...).

Thus defined, 'data localisation' in some countries constitutes a bottleneck for some Internet-enabled services and industries. Localisation strategies have thus triggered virulent opposition from corporations, civil society actors, foreign stakeholders, industry associations, and governments that have declared their support for cross-border data transfers.

Discussing the policies which undergird such obligations is beyond the remit of this Review, which is focused on improving legal certainty and enhancing compatibility between Asian frameworks on cross-border personal data flows.

However, even from this perspective alone, several observations can be made.

Improving legal certainty and predictability in the application of localisation rules

First, this area of the law is marked by uncertainty, particularly in jurisdictions where sweeping localisation obligations apply and where the state of the law is in constant flux.

As a result, organisations within the scope of such measures find themselves subject to an obligation of compliance which can be challenging to satisfy due to the legal uncertainty which prevails in this area.

In fact, we observe that over the past years, the laws and regulations imposing such obligations have been subject to constant change across the region. The unpredictability that resulted has been the cause of much disarray for companies, both local and foreign.

At least clarifying the scope and impact of such localisation measures would significantly improve the situation for organisations intending to transfer data across borders in the region, to acknowledge for the fact that the additional constraints put on the collection and processing of such data require strictly circumscribing their conditions for implementation.

52 See, for instance, Arindrajit Basu, Elonnai Hickok, and Aditya Singh Chawla, *The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India* (The Centre for Internet and Society, India; 19 March 2019) at 24.

53 Cf. the original explanatory memorandum to the OECD Privacy Guidelines, Part 3, at para. 17 (Basic principles of international application: free flow and legitimate restrictions).

In particular, this requires clarifying:

- the key concepts which underpin data localisation requirements (e.g., 'sensitive' or 'important' data); it is suggested that the list of data covered by the law should be closed and defined in the relevant statute (rather than be extendable by further regulations or other subordinate instruments);
- the circumstances in which exemptions are permitted; and so minimum transparency on the processing of exemption requests is necessary–both on the application procedure, and on precedent decisions made in similar circumstances; and
- the regulatory expectations as to the practical consequences of mandating the localisation of some categories of data (i.e. whether localisation requires server mirroring or other measures such as backup servers).

Entry into force periods should be sufficiently long to allow organisations to take the necessary compliance measures, and extensions and adaptations should be possible on request.

Combining derogations to localisation rules and data transfer mechanisms in Data Protection Laws

Second, co-existence of both types of personal data transfer restrictions (i.e., localisation requirements and data transfer provisions in the Data Protection Law) in several Asian legal systems can be a source of confusion for stakeholders.

For efforts toward legal convergence to succeed in practice, it is critically important to make explicit the purposes that these different rules serve.

Whilst the objective of aligning those data transfer requirements guided by a concern of dilution of data protection rules seems attainable, it is more elusive when data transfer restrictions are inspired by domestic concerns that do not reconcile with the promotion of compatibility among Asian data transfer frameworks.

Nevertheless, there would be great added value in the clarification of the interplay between transfer provisions in general Data Protection Laws (both the national Data Protection Law and the Data Protection Laws of other jurisdictions) and localisation obligations mandated in specific sectoral laws or regulations.

This would include, for instance, clarifying the extent of parity between 'traditional' data transfer mechanisms recognised in other jurisdictions (e.g., contracts, BCRs, certification, codes, level of protection in the country of destination, etc.) and the conditions for approval of data transfers by the public authorities.

Comparative analysis reveals that appropriate and accessible complaint and redress mechanisms should remain provided for, including effective legal remedial measures.

As well, similar and consistent standards should be applied to localisation requirements in regulations applying to different sectors.

The current Covid-19 situation has amplified the necessity of making all the clarifications suggested above.

First, driven by the urgency of the Covid-19 crisis, multinational clinical trials are more important than ever before. But localisation requirements, combined with the data transfer provisions and other requirements in multiple Data Protection Laws, pose significant barriers to compliance.[54]

Second, Business Continuity Plans (**BCPs**) rely on the capacity of offshore personnel to remotely support systems where on-shore personnel are not able to support their systems during lockdowns. Alternatively, in a worst-case scenario, the majority of personnel may become infected which results in both in-country primary and backup data centres having to go offline. The inability to process or store data offshore is a critical factor in the assessment of the risks attached to the systems going down in some jurisdictions.

[54] John Childs-Eddy, 'How to comply with data localization regulations amid COVID-19's impact', IAPP news, April 28, 2020, <https://iapp.org/news/a/how-to-comply-with-data-localization-regulations-amid-covid-19s-impact/>.

Status in Asia

Here we exclusively consider four legal systems where sweeping localisation obligations apply cross-sector to online activities (e.g. 'network providers') will impact the future data protection laws in those jurisdictions. Sectoral or targeted localisation requirements which may apply in other jurisdictions (electronic health records in Australia; tax information in New Zealand; or personal credit information in South Korea, for instance) are not considered here, except where they articulate with broader localisation requirements.

China

Cybersecurity Law (CSL) Art 37

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 requirements it is *'truly necessary'* to provide personal information outside of the PRC, CIIOs shall follow the measures of State Network Information Department and State Departments (unless laws or regulations provide otherwise) to conduct a cross-border transfer security assessment.

Personal Information Security Specification (TC260) (GB/T 35273/2020) Art 9(8)

The Specification issued by the National Information Security Standardisation Technical Committee (TC260) will enter into force on 1 October 2020.

With regard to cross-border transfers of data collected and generated in China, Art 9(8) ('Cross-border Transfer of Personal Information') only provides that 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

The draft Measures are still pending (latest version dated 13 June 2019).

The latest draft expands the scope of the transfer measures in Art 37 of the CSL to all Network Operators (not only CIIOs) and personal information.

Network operators are *'owners and administrators of networks and network service providers'* (CSL Art 76).

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 of the CSL, e.g. in banking, insurance, and credit reporting; health and genetics; online taxi booking; and location apps.[55]

Recently significant amendments were made with regard to the People's Bank of China's Personal Financial Information Protection Technical Specification ('PFI Specification') (2020)[56] and the Regulation on the management of Human Genetic Resources adopted by the State Council (2019).[57]

55 Kemeng Cai, 'Jurisdictional Report: China' in *Regulation of Cross-Border Transfers of Personal Data in Asia* (Asian Business Law Institute, 2018) at 65 (current as at May 2018).

56 People's Bank of China's Personal Financial Information Protection Technical Specification 个人金融信息保护技术规范) JR/T 0171-2020 dated 13 February 2020 <http://www.pbc.gov.cn/zhengwugongkai/127924/128038/128109/3983078/2020030414554980731.pdf>.

57 Regulation of Human Genetic Resources of the State Council (中华人民共和国人类遗传资源管理条例) No. 717 dated 28 May 2019 <http://www.gov.cn/zhengce/content/2019-06/10/content_5398829.htm>

India

Current law

Data must be stored and/or processed in India in exception to s 43A and Rule 7 of the IT Act where specific localisation requirements apply in sectors including banking, telecom, and health:[58]

- the Reserve Bank of India's Notification on 'Storage of Payment System Data' (6 April 2018);[59]
- the Department of Industrial Policy and Promotion's 'Consolidated Foreign Direct Investment Policy' (28 August 2017);[60]
- the Department of Telecommunications' Unified Access License;
- the Companies Act, 2013 and its Regulations;
- the 'Insurance Regulatory and Development Authority of India (Outsourcing of Activities by Indian Insurers) Regulations, 2017' (6 May 2017);[61] and
- the Ministry of Communications & Information Technology's 'National Telecom M2M Roadmap' (May 2015).[62]

Draft e-Pharmacy Regulations were released in 2018 which would impose that data generated or mirrored through e-pharmacy portal should be localised in India, but a final version has not been published yet.

Data Protection Bill (2019)

Sensitive personal 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)).

'Sensitive personal data' is defined in s 3(36) and includes financial personal data.

The list may be expanded by Government regulation.

Critical personal data may be processed only in India, with exceptions (s 34(2)).

'Critical personal data' is undefined and may be notified as such by Government regulation.

Indonesia

Government Regulation No.71 of 2019 (GR71) Arts 20 and 21, repealing Government Regulation No. 82 of 2012 (GR82) (October 2019)

'Electronic Service Providers (**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 (Art 20)) (subject to further implementing regulations).

'ESPs for Private Purposes' may manage, process and/or store electronic system or electronic data inside or outside Indonesia (Art 21(1)), subject to:

- the obligation to ensure effective compliance with GR71 (Art 21(2)); and
- to enable access to the data by the public authorities (Art 21(3)).

Further implementing regulations are to be provided by the Government.

58 See Amber Sinha and Elonnai Hickok, 'Jurisdictional Report: India', *ibid* at 129.

59 'Storage of Payment System Data' (Circular DPSS.CO.OD. No 2785/06.08.005/2017-18 dated 6 April 2018) <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244>.

60 Department of Industrial Policy and Promotion, 'Consolidated FDI Policy' (Effective from 28 August 2017) <https://dipp.gov.in/whats-new/consolidated-fdi-policy-circular-2017>.

61 Insurance Regulatory and Development Authority of India (Outsourcing of Activities by Indian Insurers) Regulations, 2017 (Ref No: F.No. IRDAI/Reg/5/142/2017, 6 May 2017) <https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo3149&flag=1>.

62 Ministry of Communications & Information Technology, 'National Telecom M2M Roadmap' (May 2015). <https://dot.gov.in/sites/default/files/National Telecom M2M Roadmap.pdf>. See Amber Sinha and Elonnai Hickok, 'Jurisdictional Report: India' in *Regulation of Cross-Border Transfers of Personal Data in Asia* (Asian Business Law Institute, 2018) at 129.

Further, ESPs that are deemed to have *'strategic electronic data'* (for now undefined) must backup records to *'a certain data centre'* (Art 99(3)). Regulatory guidance will be needed on the location of such data centres and whether 'Private ESPs' are included in the scope.

In the financial sector, the Financial Service Authority may adopt specific regulations relating to the transfers of personal data (Art 21(4)).

The concept of *'data categorisation'* in the previous draft of GR71 was removed from the text.

Vietnam

Cybersecurity Law, Art 26(3)

Art 26(3) of the 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 Art 26(3) are required to set up branches or representative offices in Vietnam.

Art 26(4) further provides that the Government shall provide detailed regulations on Art 26(3).

Draft Implementation Decree

A Draft Decree implementing the requirements of Art 26(3) of the CSL is expected in 2020.

Based on the latest available version of the draft (21 August 2019), storing data and/or having branches or representative offices in Vietnam is required for foreign service providers only for specific purposes, i.e. *'protection of national security, social order and safety, social ethics and health of the community*' (Chapter 5, Art 26).

There should further be legal bases for a full determination on the three following factors:[63]

- such an enterprise provides regulated services (Art 26(1)(a));
- such an enterprise carries out activities of collecting, using, analysing and processing the regulated types of data (Art 26(1)(b)); and
- such an enterprise has been notified that the service it provides is being used to commit acts of violation of Vietnamese laws, but it has not undertaken measures to stop and apprehend those acts (Art 26(1)(c)).

The regulated services and types of data (data of service users in Vietnam, generated by service users in Vietnam, and on the relationships of service users in Vietnam), the relevant authorities and the modalities of notification are further specified in the draft.

The period for the storage of data would be at least twelve (12) months (Art 27(3)).

[63] Thomas J. Treutler, Giang Thi Huong Tran, 'Update on the Implementation of Vietnam's New Cybersecurity Law and Status of Implementing Decrees', *Tilleke & Gibbins*, 18 December 2018 <https://www.tilleke.com/resources/update-implementation-vietnam%E2%80%99s-new-cybersecurity-law-and-status-implementing-decrees>.

Overarching Policy Considerations

Diversity of mechanisms to be recognised for compliance with data transfer regulations

Overall, the options for managing cross-border data transfers under data protection laws are many and varied. At the global level, *'most countries adopt a mixture of these measures and allow businesses considerable leeway in managing their own cross-border transfers'*,[64] since no single mechanism stands out as entirely positive.

Moreover, the appropriateness of a legal ground or mechanism for a given transfer scenario will depend on the context, business relationships and data use.

Contributors to ABLI's Data Privacy Project and industry generally underline the importance of ensuring that numerous mechanisms and legal bases to frame data transfers should be included in any privacy law. This diversity is part of the regulatory flexibility needed to accommodate the different economies, legal systems, and levels of development of data protection frameworks in Asia.

Convergence would be greatly facilitated by ensuring maximum overlap between Asian legal systems regarding acceptable data transfer mechanisms and schemes.

Common standards to recognize the validity of transfer mechanisms or schemes

Convergence would be advanced if the implementation of these mechanisms and schemes would be subject to comparable conditions so that they can be used for compliance in multiple jurisdictions.[65]

Data protection frameworks should recognise the validity of specific transfer instruments by applying the same 'reading grid' to all (i.e., contracts, BCRs, certification, codes of conduct, etc.), so that they provide the same safeguards, in whichever data transfer scenario they are applied.

The same criteria should be shared across legal systems in order to promote legal certainty, convergence and interoperability.

Broadly put, Asian laws combined with available guidance provide that any data transfer mechanism should ensure a continuing level of protection overseas, consistent with international data protection and privacy standards as well as the objects of the national data protection law.

With regard to data transfers, comparative analysis of Asian laws, combined with international data protection standards, leads to the conclusion that:

- any data transfer mechanism must consist in a legally binding arrangement;
- any data transfer mechanism must maintain and build upon the existing privacy protections set out in the national legislation, while being consistent with principles enshrined in international frameworks and best practices;
- data subjects' rights must remain enforceable overseas; this implies that appropriate and accessible complaint and redress mechanisms are provided for, including effective legal remedial measures; and
- adequate supervisory mechanisms must apply to the scheme or instrument to ensure effective compliance of transferring organisations with their obligations under national laws.

Enforcement mechanisms

An enforcement mechanism should meet two key requirements:

- it should be accessible to the individual; and
- it should have effective powers to enforce the privacy or data protections in the legally binding arrangement.

64 UNCTAD report, 'Data protection regulations and international data flows', *ibid* at 14.

65 Park Kwang Bae, 'Jurisdictional Report: Republic of Korea', *ibid* at 369.

It is understood that a range of mechanisms may satisfy those requirements, ranging from a regulatory body similar to the local data protection regulator, to an accredited dispute resolution scheme, an independent tribunal or a court with judicial functions and powers.[66]

Factors that may be relevant in deciding whether there is an effective enforcement mechanism include whether the mechanism:[67]

- is independent of the overseas recipient that is required by the law or binding scheme to comply with the privacy or data protections;
- has authority to consider a breach of any of the privacy or data protections in the arrangement;
- is accessible to an individual, for example, the existence of the arrangement is publicly known, and can be accessed by individuals directly and without payment of any unreasonable charge;
- has the power to make a finding that the overseas recipient is in breach of the arrangement and to provide a remedy to the individual; and
- is required to operate according to principles of procedural fairness.

The mechanism may be a single mechanism or a combination of mechanisms. It may be established by the law or binding scheme that contains the privacy or data protections, or by another law or binding scheme.

Alternatively, the mechanism may take effect through the operation of cross-border enforcement arrangements between the appropriate regulatory authorities.

Alignment on global standards

Finally, an important assumption shared by ABLI's interlocutors is that neither regulatory competition, nor simplification should be done at the expense of privacy itself.

Like security and accountability, data protection and privacy are a central component of digital trust, the keystone on which the digital evolution and the productive use of new technologies rest,[68] so it must now be taken for granted that sustainable convergence in this area of law will only be achieved if a high level of data protection and privacy is implemented in the legal systems of the region.

Alignment not just to a regional standard but to global standards is a worthwhile goal, especially given the integration of Asian economies in global trade and the increased privacy expectations of the Asian public.

Ensuring consistency between global, regional and sub-regional frameworks is necessary to avoid adding more layers of complexity.

66 OECD Privacy Framework, Para 17(b), p.30.

67 OAIC APP 'Guidelines, Chapter 8: APP 8 — Cross-border disclosure of personal information', on 'Mechanisms to enforce privacy protections', p.9.

68 Bhaskar Chakravorti and Ravi Shankar Chaturvedi, 'Digital Planet 2017: How Competitiveness and Trust in Digital Economies Vary Across the World', The Fletcher School, Tufts University, July 2017, p. 28.

Acknowledgments

The Asian Business Law Institute is indebted to the following Data Protection and Privacy Commissions that have expressed their support of this Review, and provided comments or clarifications on their respective national frameworks:

- Office of the Australian Information Commissioner (**OAIC**), Australia;
- Privacy Commissioner for Personal Data (**PCPD**), Hong Kong SAR;
- Personal Information Protection Commission (**PIPC**), Japan;
- Office for Personal Data Protection (**OPDP**), Macau SAR;
- Office of the Privacy Commissioner (**OPC**), New Zealand;
- National Privacy Commission (**NPC**), Philippines;
- Personal Data Protection Commission (**PDPC**), Singapore; and
- Personal Information Protection Commission (**PIPC**), South Korea.

With special thanks for their personal contributions to: Emi Christensen, Aleksandra The-Tjoan, Aki Cheung, Mari Sonoda, Ken Chongwei Yang, Michael Harrison, Leandro Angelo Aguirre, Angela Butalid, Evelyn Goh, Eunice Lim, and Huynik Kim.

This Review was edited with the invaluable assistance of Dominic Paulger.

We gratefully acknowledge the individual contributions of Charmian Aw (Reed Smith, Singapore), Kemeng Cai (Han Kun Law, China), Dr Yanqing Hong (Peking University, China), Mark Parsons (Hogan Lovells, Hong Kong), Elonnai Hickok (Center for Internet and Society, India), Danny Kobrata (K&K Advocates, Indonesia), Deepak Pillai (Christopher & Lee Ong, Malaysia), Jj Disini (Disini Law Office, Philippines), Ken Chia (Baker & Mc Kenzie, Singapore), Park Kwang Bae (Lee & Ko, Korea), David Duncan (Tilleke & Gibbins, Thailand), Prapanpong Khumon (Chulalongkorn University, Thailand), Waewpen Piemwichai (Tilleke & Gibbins, Vietnam), Derek Ho, Annabel Lee, Eric Chung, Marcus Bartley-Johns, Alex Li, and Larry Liu.

All responsibility for content remains with the Asian Business Law Institute.

Asian Business Law Institute

The Asian Business Law Institute is a neutral, non-profit permanent institute based in Singapore dedicated to providing practical guidance in the field of Asian legal development and promoting the convergence of Asian business laws.

The Asian Business Law Institute seeks to address key problems resulting from legal diversity in Asia identified by stakeholders in the public and private sectors. ABLI's long-term strategic direction is set by a Board of Governors, chaired by the Honourable the Chief Justice Sundaresh Menon of the Supreme Court of Singapore. The Board of Governors comprises representatives of the judiciaries of Australia, China, Singapore and India and other internationally renowned legal experts.

Since 2017, the Asian Business Law Institute has undertaken a multi-stakeholder project focusing on the regulation of international data transfers in 14 Asian jurisdictions, in collaboration with a wide range of stakeholders including law practitioners, industry representatives and academics, and with input from the Data Protection and Privacy Commissions and governments of the region which are currently working on, or reviewing, their respective data protection frameworks.

The Data Privacy Project is led by Dr Clarisse Girot, Senior Fellow with the Asian Business Law Institute.

More information on the Project is available at https://abli.asia/.