ISSUE BRIEF

GLOBAL

Navigating Cross-Border Data Transfers in the Asia-Pacific Region (APAC)

Analyzing Legal Developments from 2021 to 2023

Author: Dominic Paulger, FPF, September 2023

FUTURE OF PRIVACY FORUM

Contributors

Contributors:

- **Kemeng Cai (China)**
- **Iqsan Sirie and Daniar Supriyadi (Indonesia)**
- **Takeshige Sugimoto (Japan)**
- **Thitirat Thipsamritkul (Thailand)**
- **Kwang Bae Park (South Korea)**
- **Kat MH Hille (Vietnam)**

This Issue Brief benefited from contributions from FPF Global Privacy interns Pang Cheng Kit and Raktima Roy and contributions and editing support from Lee Matheson and Josh Lee Kok Thong.

Table of Contents

Introduction

The landscape for cross-border data transfers in the Asia Pacific region (APAC) has changed rapidly as several APAC jurisdictions have either enacted new data protection laws or undertaken major reviews of existing data protection laws and regulations.

China, Indonesia, and Vietnam enacted comprehensive national data protection legislation in 2021, 2022, and 2023, respectively. In 2022, Thailand's first comprehensive data protection law took effect, following delays due to the COVID-19 pandemic. Early in 2023, South Korea passed the most expansive amendments to its data protection law to date, including several changes to its provisions on cross-border data transfers.

There have also been substantial developments in regional and international initiatives to promote interoperability between data protection laws and facilitate cross-border data transfers. For instance, in 2021, the Association of Southeast Asian Nations (ASEAN) released a set of Model Contractual Clauses (MCCs) that private-sector entities may choose to include or adapt for use in legal agreements for transfers of personal data between ASEAN member states. In 2022, several members of the Asia-Pacific Economic Cooperation (APEC) agreed to establish the Global Cross-Border Privacy Rules Forum with a view to develop and promote an international certification system for cross-border data transfers based on the APEC Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) Systems. 2023 has also seen Japan promote and seek to operationalize the concept of "Data Free Flow with Trust" through its presidency of the Group of Seven (G7) member states.

This Issue Brief outlines the key developments in cross-border data transfers in APAC in the last few years and explores the potential impact on businesses that operate in the APAC region.

Background

In today's interconnected world, cross-border data transfers play a pivotal role in driving the global digital economy and facilitating digital trade. The ability to seamlessly transfer personal data across borders enables businesses to provide services on an international scale and provides individuals with access to a wide range of digital services and platforms that can promote collaboration and innovation.

However, despite their benefits, cross-border data transfers raise legitimate concerns regarding the protection of individuals' privacy, data security, and the potential misuse of their personal data. Data protection laws therefore attempt to strike a balance between facilitating cross-border data transfers and safeguarding individuals' rights and interests. As a result, data protection laws commonly require organizations to satisfy certain conditions before they may legally transfer personal data out of the jurisdiction where the data is stored. The aim of these

requirements is generally to ensure that personal data is appropriately protected when it is transferred out of the jurisdiction, absent special circumstances.

Common conditions include the following:

1. Assessment of the Level of Personal Data Protection in the Destination Jurisdiction (Adequacy)
Many data protection laws internationally permit the transfer of personal data to other jurisdictions if the legal frameworks of the destination protect personal data to a comparable or equivalent level to that of the source jurisdiction.

Often, these laws establish a mechanism for the data protection authority to assess the adequacy of other jurisdictions' data protection frameworks and issue decisions which function as a "whitelist" of destinations to which transfers of personal data are permitted. For example, Article 45 of the EU's GDPR permits transfers of personal data to a jurisdiction which the European Commission has determined ensures an "adequate level of protection" of personal data.

2. Adoption of Safeguards
Many data protection laws internationally also permit the transfer of personal data to other jurisdictions if the transferor provides the personal data with appropriate safeguards.

These safeguards commonly take the form of **legally binding agreements** between the transferor and recipient specifying that the recipient will adopt particular measures to protect the personal data following the transfer. Several jurisdictions (including the EU, Hong Kong, New Zealand, and most recently, China) and supranational organizations (including ASEAN) have released model or standard contractual clauses (SCCs) for this purpose.

The safeguards may also take the form of **certifications or rules approved by the regulator**. For example, Article 46 of the GDPR enables transfers of Europeans' personal data out of the EU on the basis of approved binding corporate rules (BCRs) adopted by groups of related businesses, certifications, and codes of conduct. Within participating members, the APEC CBPR system functions as a voluntary certification scheme in which an independent assessor assesses businesses' compliance with a set of agreed privacy principles.

3. Consent
Many data protection laws internationally also permit the transfer of personal data to other jurisdictions if the data subject has consented to the transfer.

Typically, these laws (including the GDPR) also impose notification and transparency obligations on the transferor to ensure that the data subject is aware that their personal data may not be protected to a comparable standard following the transfer (or else any consent obtained by the transferor may be rendered invalid).

Some laws may also require that the transferor adopt safeguards to protect the personal data even if the data subject has provided valid consent.

4. Necessity

Some data protection laws also permit transfers of personal data to other jurisdictions in exceptional circumstances where the transfer is necessary for an important interest, such as the life or health of another person, public interest concerns, or execution or performance of a contract between the transferor and data subject or in the data subject's interest.

It is important to note that in most jurisdictions these options are provided for not as equal alternatives available to data exporters but rather, within a hierarchy of available grounds.

Trends in the APAC Region

Divergences in Legal Bases for Cross-Border Transfers of Personal Data

In the APAC region, where diverse legal systems and cultural contexts intersect, navigating the landscape of cross-border data transfers poses unique challenges for businesses that operate in multiple jurisdictions. A 2020 study by the Asian Business Law Institute (ABLI) found that the regulatory landscape for cross-border data transfers in the APAC region was fragmented and would benefit from efforts to promote legal certainty and interoperability of regional laws and regulations.

However, since this study was published, several major new data protection laws have been enacted in APAC. As a result, the majority of APAC jurisdictions now have comprehensive data protection laws. Most of these laws provide organizations with several different options (such as adequacy, adoption of safeguards, or consent) to legally transfer personal data to other jurisdictions.

A review of six data protection laws that have been enacted, amended, or have come into force since 2021 (**China**, **Indonesia**, **Japan**, **South Korea**, **Thailand**, and **Vietnam**) indicates that there is a degree of alignment between Indonesia, Japan, South Korea, and Thailand regarding legal bases for cross-border data transfers, but China and Vietnam are outliers with their own unique requirements.

Indonesia, Japan, South Korea, and Thailand all recognize adequacy and consent as valid legal bases for cross-border data transfers. There is also some alignment on recognition of certification schemes. However, as many of these laws were enacted or amended very recently, there remains uncertainty as to which jurisdictions might be recognized as mutually adequate, or which certification schemes will ultimately be recognized. As a result, organizations operating in these jurisdictions may find it easier to organize their cross-border data transfer compliance efforts around consent.

China and Vietnam both differ substantially from the other jurisdictions studied. Both China and Vietnam impose unique conditions for transferring personal data, including requiring transferring organizations to undertake and file detailed assessments with the relevant regulator. Vietnam recognizes only a single legal basis for transferring

personal data out of the country, while China recognizes three – although there is significant overlap in the filing requirements for the three options under Chinese law.

The following table provides a side-by-side comparison of the six jurisdictions for a number of key cross-border data transfer concepts. More details about each jurisdiction will be provided in one of the three annexes to this Issue Brief: Annex 1 - China; Annex 2 - Southeast Asia; Annex 3 - Northeast Asia.

Table 1. An overview of cross-border data transfer provisions in the data protection laws and regulations of China, Indonesia, Japan, South Korea, Thailand, and Vietnam

	China	Indonesia	Japan	South Korea	Thailand	Vietnam
Adequacy	**No.**	**Yes.** However, there is currently no clear mechanism for determining if another jurisdiction provides an adequate level of data protection.	**Yes.** To date, only the EU and the UK have been determined to provide an adequate level of data protection.	**Yes.** Recent amendments to South Korea's data protection law have introduced adequacy as a legal basis for cross-border transfers of personal data. Given that South Korea has an EU adequacy decision, it is possible that South Korea will reciprocally recognize the EU as providing an adequate level of data protection.	**Yes.** However, there is currently no clear mechanism for determining if another jurisdiction provides an adequate level of data protection.	**No.**

Certification	**Yes.**	**Possible.** While Indonesia's data protection law does not refer to certification schemes, it is possible that certification schemes could be recognized under "adequate and binding safeguards."	**Yes.** Japan's data protection law recognizes a legal basis for cross-border transfer of personal data in the absence of adequacy if the overseas recipient of the personal data has established a system that provides equivalent protection to that under Japanese law. The APEC CBPR system has been recognized for this purpose.	**Yes.** South Korea's data protection law recognizes a legal basis for cross-border transfer of personal data if the transferor has received a certification from South Korea's data protection authority.	**Yes.** Thailand's data protection law recognizes a legal basis for cross-border transfers of personal data if the transferor has put in place a personal data protection policy governing the transfer, and the policy is reviewed and certified by Thailand's data protection authority.	**No.**
Consent	**No.** Consent is not an independent legal basis for cross-border transfers of personal data. However, consent may still be required in some cases.	**Yes.** The transferor must satisfy specific notice requirements for consent to be a valid legal basis for cross-border transfers of personal data.	**Yes.** The transferor must satisfy specific notice requirements for consent to be a valid legal basis for cross-border transfers of personal data.	**Yes.** The transferor must satisfy specific notice requirements for consent to be a valid legal basis for cross-border transfers of personal data.	**Yes.** The transferor must satisfy specific notice requirements for consent to be a valid legal basis for cross-border transfers of personal data.	**No.** Consent is not an independent legal basis for cross-border transfers of personal data. However, consent may still be required in some cases.

Filing a security assessment with the regulator	**Yes.** In China, the most stringent security assessment is only required if the transferor: (1) transfers prescribed classes of "important data;" (2) is a critical information infrastructure operator; (3) processes the personal data of > 1 million people; (3) has, in the last year, transferred more than a prescribed volume of personal data out of China. However, for all cross-border transfers of personal data, the transferor must undertake a data protection impact assessment and file this with the regulator.	**No.**	**No.**	**No.**	**No.**	**Yes.** The sole legal basis for transferring personal data out of Vietnam requires the transferor to undertake a stringent security assessment and file a copy of the assessment with the regulator.

Necessity for performance of a contract with the data subject	**No.**	**No.**	**No.**	**Yes.** South Korea's data protection law recognizes a legal basis for cross-border transfer of personal data where the transfer is necessary for performance of a contract with the data subject.	**Yes.** Thailand's personal data law recognizes a legal basis for cross-border transfer of personal data where the transfer is necessary for performance of a contract with the data subject.	**No.**
Other necessity	**No.**	**No.**	**Yes.** Japan's data protection law recognizes legal bases for cross-border transfer of personal data where the transfer is necessary to protect a person's vital interests or public health or for various academic research purposes.	**No.**	**Yes.** Thailand's personal data law recognizes a legal basis for cross-border transfer of personal data where the transfer is necessary for various purposes, which are similar to those recognized under the GDPR.	**No.**

Other safeguards in absence of adequacy or certification	**No.** China's data protection law requires the transferor to implement certain safeguards, but these requirements apply regardless of the level of data protection provided by the destination jurisdiction.	**Yes.** Indonesia's data protection law recognizes a legal basis for cross-border transfer of personal data in the absence of adequacy if there are "adequate and binding safeguards." The scope of this provision remains unclear but may be clarified in future regulations.	**No.**	**No.**	**Yes.** Thailand's data protection law recognizes a legal basis for cross-border transfer of personal data in the absence of adequacy or certification if the transferor implements suitable protection measures which enable the enforcement of the data subject's rights, including effective legal remedial measures according to the rules and methods to be prescribed by Thailand's data protection authority.	**No.**

Divergence in approaches to regulation of cross-border data transfers likely reflects different policy considerations in every jurisdiction, as well as different notions of the value of personal data. In particular, there appears to be a tension between demands (often made by international business) to align with influential data protection frameworks like the GDPR on one hand, and respect for local considerations, such as protecting national security and sovereignty, and safeguarding the local economy from external risks and competitors, on the other hand. In some cases, this tension has produced structures that are GDPR-like but not entirely GDPR-compatible. This may complicate efforts by organizations that operate in multiple jurisdictions to align their compliance programs, which are often based on the GDPR, with requirements in the APAC region.

Divergences at the Implementation Level

In addition to differences in legal bases for transferring personal data across borders, this review has also revealed that there are differences in the level of legal guidance around the use of these bases. For jurisdictions like **Indonesia**, **Thailand,** and **Vietnam**, whose data protection laws were only recently enacted, there is still a lack

of clarity on how authorities will interpret key provisions as these authorities have not yet issued implementing regulations and guidelines for these provisions.

Growth in Standardized Contractual Language for Cross-Border Data Flows

The ABLI's 2020 study of cross-border data transfer regulations in the APAC region suggested that contractual safeguards could become a promising avenue for increasing the interoperability of regional data protection frameworks, particularly if regional regulators could agree on shared contractual data privacy and security controls.

In the years following the ABLI study, **China** has released regulations and guidelines on binding SCCs for cross-border data transfer, and **ASEAN** released its voluntary MCCs for private-sector organizations to use as a framework to transfer personal data between ASEAN member states. While **China**'s SCCs may be the most readily available mechanism for most businesses to transfer personal information out of the PRC, the utility of ASEAN's voluntary MCCs is still unclear. In the Philippines and Singapore, regulators have provided guidance on the role of the ASEAN MCCs in cross-border data transfers. However, in other major ASEAN economies **Indonesia, Thailand**, and **Vietnam,** which have recently enacted comprehensive personal data protection laws, it remains unclear whether organizations would be able to rely on the ASEAN MCCs as regulators in these jurisdictions have not yet provided guidance on whether the MCCs meet the requirements of relevant cross-border data transfer provisions, especially those permitting data transfers based on appropriate safeguards.

Interoperability with established binding frameworks in other jurisdictions is a significant factor in whether businesses adopt voluntary frameworks like the ASEAN MCCs. To date, there have been some efforts to compare and map the requirements of the MCCs with other contractual frameworks, such as FPF's study mapping the ASEAN MCCs to the EU's SCCs and the Iberoamerican Network's Model Transfer Agreement), and more recently, the European Commission and ASEAN's "Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses."

Possibility of EU Adequacy

EU adequacy status in APAC has been limited. Of the 6 jurisdictions reviewed in this article, only **Japan** and **South Korea** have obtained adequacy decisions from the European Commission. While the remaining 4 jurisdictions – **China**, **Indonesia**, **Thailand**, and **Vietnam** – have data protection laws which align to some extent with the GDPR, these data protection frameworks are still relatively new and would likely require further development and implementation before conversations on EU adequacy status can begin.

Annex 1: People's Republic of China (PRC)

In recent years, China has rapidly established a legal framework governing the processing of personal information (PI), including transfers of PI out of the PRC.

This process began with the Cybersecurity Law (CSL) – China's first national law with provisions covering personal data protection – which was enacted in 2016 and became effective on June 1, 2017. The CSL was followed by enactment of the Data Security Law (DSL) in June 2021 and the Personal Information Protection Law (PIPL), China's first comprehensive data protection law, in August 2021.

The CSL, DSL, and PIPL are three primary laws that make up China's regulatory framework for protecting data, including but not limited to PI. Since 2021, the Cyberspace Administration of China (CAC) – the state body responsible for administering the CSL, DSL, and PIPL – has also released several subsidiary regulations implementing specific requirements under the primary laws.

The CSL sets out a general requirement for "critical information infrastructure operators" (CIIO) to conduct a security assessment before transferring PI or other "important data" out of the PRC. These terms are not defined in the CSL, but their scope has been developed through subsidiary regulations (see below).

The PIPL builds significantly on the foundation in the CSL and provides four legal bases for organizations that process PI (known as "PI handlers" in the PIPL) to transfer PI out of the PRC. These include:

1. Passing a **security assessment** by the CAC.
2. Undergoing **certification** by a specialized body according to rules provided by the CAC.
3. Concluding a contract with the overseas recipient of the PI using a **standard contract** provided by the CAC.
4. Meeting other conditions provided in laws or regulations or required by the CAC.

Note that passing a security assessment is the only legal basis for cross-border transfer of PI by CIIOs, or by PI handlers which process or transfer PI exceeding the volume threshold provided by the CAC (see below).

According to the CAC's official guidelines on data export security assessments, the following would be considered cross-border transfers of data:

- Transfer by data handlers of data collected and generated in the course of their domestic operation outside of China;
- Allowing overseas institutions, organizations, or individuals to search, access, download, and retrieve data that data handlers store within the PRC; and
- Any other data export activities prescribed by CAC.

Adequacy

The PIPL does not provide for a GDPR-style adequacy regime.

Adoption of Safeguards

Regardless of which legal basis a transferor relies on, the PIPL requires PI handlers to:

- Conduct a PI protection impact assessment before transferring the PI out of the PRC; and
- Adopt necessary measures to ensure that the recipient protects the PI to a comparable level to that required by the PIPL.

Consent

The PIPL does not recognize consent as an independent legal basis for transferring PI out of the PRC. A PI handler must still satisfy the requirements of one of the above legal bases for cross-border data transfer before it may transfer PI out of the PRC.

However, a PI handler may still be required to obtain separate consent to transfer PI out of the PRC, if the PI was originally collected on the basis of consent. In order to obtain separate consent, the PI handler must provide individuals with the following information:

- The name and contact information of the overseas recipient;
- The purpose and method of processing;
- The categories of PI that will be processed; and
- The measures and procedures for individuals to exercise their PI rights against the overseas recipient of the data.

Security Assessment

This basis for cross-border data transfers is regulated by the CAC's Measures for the Security Assessment of Outbound Data Transfers (Security Assessment Measures), which became effective on September 1, 2022. The Security Assessment Measures were accompanied by the release of a set of guidelines by the CAC providing further detail on the application process and procedures for a security assessment.

Security assessment is only mandatory where:

- The transfer involves "important data" (i.e., data that may endanger national security, economic operation, social stability, public health, and safety, etc. if it is tampered with, destroyed, leaked, illegally obtained or used);
- The transferor is a CIIO;
- The transferor processes the PI of more than 1 million people;
- The transferor has, since January 1 of the preceding year, transferred the PI of 100,000 people or the sensitive PI of 10,000 people out of the PRC;
- Other circumstances stipulated by the CAC.

The Security Assessment Measures require data handlers to enter into a legally binding agreement with the overseas recipient setting out the recipient's rights and obligations in relation to the PI, including in the following areas:

- The purpose, method, and scope of the transfer and subsequent processing;
- The location and period for storing the data;
- Processing of the data once the agreed storage period expires, the agreed purpose is fulfilled, or the agreement is terminated;
- Binding restrictions on onward cross-border data transfers;
- Security measures to be taken when:
    - there are changes to:
        - the recipient's ownership or scope of business;
        - the data and network security policies and regulations of the jurisdiction where the data is stored;
    - a force majeure event occurs which makes it difficult to guarantee the security of the data;
- Remedial measures, liability for breach of contract, and dispute resolution methods for violations of data security protection obligations; and
- Obligations regarding emergency response and ways and means to protect the rights and interests of individuals when the data is tampered with, destroyed, leaked, lost, or otherwise illegally used.

Before applying for security assessment for an outbound data transfer, the transferor must undertake a self-assessment of risks from the data transfer, focusing on:

- The legality, legitimacy, necessity of the transfer;
- The purpose, scope, and method of data processing by the overseas recipient;
- The scale, scope, type, and sensitivity of the outbound data;
- The risks of the data transfer to national security, public interests, and the legitimate rights and interests of individuals or organizations;
- The responsibilities and obligations that the overseas recipient has agreed to adopt, and whether the recipient has the management and technical measures and capabilities to fulfill these responsibilities and obligations to guarantee the security of the data;
- The risk of data being tampered with, destroyed, leaked, lost, transferred, or illegally acquired or used during and after the data is exported, and whether the channels for the protection of PI rights are unobstructed, etc.;
- Whether the legally-binding agreement between the transferor and the recipient;
- Any other relevant matters.

The transferor must provide the self-assessment, together with the legal document to be concluded between the data handler and the overseas recipient, for inspection and security assessment, which focuses on assessing the risks that the transfer may bring to national security, public interests, and the legitimate rights and interests of individuals or organizations, mainly including:

- The legality, legitimacy, and necessity of the purpose, scope, and method of data exportation;
- The impact of the data security protection policies and regulations of the country or region where the overseas receiver is located and the network security environment on the security of outbound data; whether the data protection level of the overseas receiver meets the provisions of the laws and administrative regulations of the PRC and mandatory national standards requirements;

- The scale, scope, type, and sensitivity of the outbound data, and the risks of tampering, destruction, disclosure, loss, transfer, or illegal acquisition or use of the outbound data during and after the outbound data;
- Whether data security and PI rights and interests can be fully and effectively guaranteed;
- Whether the legal documents to be concluded between the data handler and the overseas recipient fully stipulate the responsibility and obligation for data security protection;
- Compliance with Chinese laws, administrative regulations, and departmental rules;
- Other matters deemed necessary by the national cyberspace administration.

A security assessment lasts for 2 years from the date when the result is issued. Reevaluation is necessary if there are changes in the criteria for evaluation.

Analysis: Security assessment would not be the first choice for businesses as it has the strictest requirements of the three legal bases for transferring PI under the PIPL. Nevertheless, many businesses may still be caught by the mandatory requirement to undertake a security assessment for cross-border data transfers as the threshold condition of processing the PI of at least one million users in China is fairly easy to meet, given the size of the Chinese market.

For CIIOs, Chinese regulators notify the operator in key industries and sectors if they determine that such operators are CIIOs. The Critical Information Infrastructure Security Protection Regulations issued by the CAC in August 2021 define "critical information infrastructure" expansively to include public communication and information services, energy, transportation, water conservancy, finance, public services, e-government, national defense, science and technology industry and other important industries and fields, but also other infrastructure that in the event of damage, loss of function, or data leakage, may seriously endanger national security, national economy and people's livelihood, as well as important network facilities and information systems of public interest.

For other businesses that do not fall within the above groups, there may be uncertainty as to whether they process "important data" and are therefore also subject to mandatory security assessment requirements. Chinese authorities have wide discretion in determining the scope of "important data" and for now, there is a lack of clear guidance. The identification of important data is mainly carried out by industrial regulators and local authorities, and some authorities have promulgated regulations or guidelines for the identification of important data in the relevant industries or regions, for example, the regulations on important data in industry and informatization areas, automobile areas, and the pilot identification program in Shanghai.

Chinese regulators are also in the process of formulating guidelines on identification of important data. The National Information Security Standardisation Technical Committee (also known as TC260) released a draft guideline on identification of "important data" for public consultation in January 2022. However, this guideline is brief, and it remains to be seen whether it will be developed into a more comprehensive draft and enacted.

Certification

Certification is an optional procedure for businesses that process PI.

To date, the CAC has only authorized a single body, the China Cybersecurity Review Technology and Certification Center (a state-owned certification institution under the supervision of the State Administration for Market Regulation (SAMR)), to undertake and issue certifications. The Center has publicized its procedure for accepting applications for certification but has not yet released the result of any ongoing certification applications. Certification is valid for 3 years, subject to ongoing supervision by the certification body.

In November 2022, the CAC and the SAMR released the "Implementation Rules for PI Protection Certification" (Certification Rules), which set out the high-level requirements for certification of PI processing activities, including the certification process (comprising technical verification, on-site review, and evaluation) and ongoing supervision after certification has been granted.

The Certification Rules specify that PI handlers who wish to transfer PI out of the PRC will be assessed against the latest version in force of two Chinese technical standards:

- "Information Security Technology PI Security Code" (GB/T 35273); and
- "Security certification specifications for cross-border processing of PI" (TC260-PG-20222A).

TC260-PG-20222A sets out the principles and basic requirements for certification of PI protection in the context of cross-border processing activities. Broadly, the standard requires both the PI handler and the overseas recipient of PI to:

- Enter into a legally binding agreement;
- Within their respective organizations, appoint PI protection officers and bodies to undertake functions relating to protection of PI;
- Specify rules for cross-border transfer of PI; and
- Recognize and facilitate the exercise of data subjects' rights under the PIPL, including providing information relevant to the cross-border transfer of the data subject's personal data pursuant to the data subject's right to be informed.

The PI handler must also conduct a PI protection impact assessment (PIPIA). The resulting report must be retained for a minimum of 3 years.

However, on March 10, 2023, China's National Information Security Standardisation Technical Committee of China (TC260) released a draft "Certification Requirements for Cross-Border Transmission of PI on Information Security Technology" (Draft Certification Requirements) for public consultation. This draft, which is subject to change following the public consultation, is nearly identical to TC260-PG-20222A, except for a few additional clarifications as to definitions.

Analysis: Though Chinese authorities have established the certification mechanism, it may take some time for this regime to be fully operational, and it is as yet unclear how effective this mechanism will be for transferring PI out of

the PRC, compared with the standard contract clause mechanism. Businesses may wish to closely monitor the development of this mechanism.

Commentators have drawn comparisons between the PIPL's certification mechanism and the Binding Corporate Rules mechanism in the EU's GDPR as both mechanisms would enable cross-border transfers of PI within a group of related business organizations without the need for separate agreements between the transferor and overseas recipient. However, it should be noted that TC260-PG-20222A still requires the transferor and the receiver to enter into a legally binding and enforceable document, which usually takes the form of a contract.

Standard Contractual Clauses

In February 2023, the CAC released the Standard Contract Measures for the Cross-Border Transfer of PI (Standard Contract Measures), together with a set of standard contractual clauses. The Standard Contract Measures, which outline the requirements for organizations to rely on the SCCs, took effect on June 1, 2023, with a grace period of 6 months for PI handlers to comply.

Two days before the SCC Measures took effect, the CAC released a set of guidelines, the "Guidelines for Filing Standard Contracts for Outbound Cross-Border Transfers of Personal Information" (SCC Guidelines), which provide further detail on organizations' obligations under the SCC Measures.

The SCCs are an optional mechanism available to PI handlers that are not required to conduct a mandatory security assessment (see above). Notably, the Standard Contract Measures prohibit PI handlers from circumventing the thresholds for security assessment (see above) by using several different legal entities to transfer smaller volumes of PI out of the PRC.

In order to rely on the SCCs, PI handlers must enter into a legally binding agreement with the overseas recipient containing the latest version in force of the SCCs issued by the CAC. The current version contains a total of 9 articles spanning:

- Definitions;
- Obligations of PI handlers;
- Obligations of overseas recipients;
- Declarations and guarantees regarding the policies and regulations for protection of PI in the jurisdiction where the overseas recipient is located;
- Provision on the rights of data subjects;
- Remedies;
- Termination of the agreement;
- Liability for breach of the agreement; and
- Other matters, including governing law and fora for disputes.

PI handlers may agree on other terms with the overseas recipient, but these terms must not conflict with the SCCs.

Additionally, the PI handler must conduct a PIPIA focusing on the following areas:

- The legality, legitimacy, and necessity of the purpose, scope, and method of processing PI by the PI processor and the overseas recipient.
- The scale, scope, type, and sensitivity of the PI to be transferred, and the risks that the transfer of PI may bring to data subjects' rights and interests regarding their PI.
- Whether the overseas recipient has promised to undertake certain obligations to secure the PI, and whether it has the management and technical measures and capabilities to fulfill those obligations.
- The risk of PI being tampered with, destroyed, leaked, lost, or illegally used after leaving the PRC, and whether there are straightforward channels for protecting the rights and interests of PI.
- The impact of the PI protection policies and regulations of the country or region where the overseas recipient is located on the performance of the standard contract.
- Other matters relevant to the security of the PI to be transferred out of the PRC.

Annex 5 to the SCC Guidelines provides a PIPIA template.

Within 10 working days from the date when the standard contract takes effect, the PI handler must submit:

- The contract;
- A PIPIA undertaken in the last three months; and
- A letter of undertaking (Annex 3 to the SCC Guidelines provides a template) to the local provincial CAC department. The CAC will review the application and within 15 working days, indicate whether the application passes or fails. In the latter case, the CAC will provide reasons for the rejection and an opportunity to submit supplementary information or documents within 10 working days.

If there is a change in certain prescribed matters during the validity of the contract, the PI handler must conduct a new impact assessment and if necessary, supplement the agreement or enter into a new agreement. These circumstances include changes to:

- The purpose, scope, category, degree of sensitivity, method, and storage location of PI transferred out of the PRC;
- The purpose and method of processing PI by the overseas recipient;
- The period for storing the PI outside of the PRC; and
- The PI protection policies and regulations in the country or region where the overseas recipient is located may affect the rights and interests of PI, as well as any other circumstances that may affect the rights and interests of PI.

Analysis

SCCs are the mechanism that most PI handlers will likely rely on to transfer PI out of the PRC. However, in practice, it may still be necessary for PI handlers to adapt their business practices to meet the requirements of China's SCCs given the lack of flexibility in China's SCCs, which must be adopted in their entirety by both the PI handler and the overseas recipient.

Note that unlike the EU's SCCs, or the ASEAN MCCs, China's SCCs do not differentiate between controller-to-controller or controller-to-processor transfers and instead, adopt a "one-size-fits-all" approach consisting of a single form that must be signed by both the China-based PI handler and the overseas recipient.

Penalties

The PIPL does not prescribe specific penalties for non-compliance with cross-border data transfer requirements.

However, the PIPL provides generally that where a PI handler processes PI in violation of the PIPL, the CAC may:

- Order the PI handler to correct its conduct (failing which, the handler faces an additional fine of up to 1 million RMB);
- Confiscate unlawful income; and
- Order the PI handler to cease or terminate processing of PI.

If the circumstances of the impugned act are "grave," then the CAC is additionally empowered to:

- Issue fines of:
    - up to 50 million RMB or 5% of the PI handler's annual revenue on the PI handler; and
    - between 100,000 and 1 million RMB on responsible persons;
- Order the suspension of related business activities or cessation of business for rectification;
- Report to the relevant authorities for cancellation of administrative or business licenses; and
- Prohibit responsible persons from holding senior managerial or data protection related positions for a certain period.

Annex 2: Southeast Asia

Southeast Asia's data protection landscape is emerging but has evolved significantly in recent years.

At the national level, several major economies in the region have recently adopted first-of-their-kind comprehensive national data protection laws.

- **Thailand** enacted its Personal Data Protection Act in May 2019. The Act only took full effect in May 2022.
- **Indonesia** enacted its Personal Data Protection Law in October 2022. The Law will take effect in October 2024.
- **Vietnam** enacted its Personal Data Protection Decree in April 2023. The Decree took effect in July 2023.

Provisions on cross-border data transfers in these laws are explained below.

At the regional level, there have also been several initiatives to promote interoperability between national data protection laws and facilitate cross-border data flows.

ASEAN

In 2016, the ASEAN members adopted the ASEAN Framework on Personal Data Protection (PDP Framework), a set of voluntary and non-binding principles that are intended to strengthen the protection of personal data in ASEAN and to facilitate cooperation among ASEAN member states, with a view to contribute to the promotion and growth of regional and global trade and the flow of information.

In December 2018, telecommunications and information technology ministers of the ASEAN member states adopted the ASEAN Framework on Digital Data Governance (DDG Framework), which sets out the strategic priorities, principles, and initiatives to guide member states' policy and regulatory approaches towards data governance in the digital economy. The DDG Framework identifies cross-border data flows as a key strategic priority and encourages ASEAN member states to increase legal certainty, and avoid imposing unnecessary restrictions, on cross-border data flows.

In January 2021, digital ministers from the ASEAN member states adopted the previously mentioned ASEAN MCCs: a voluntary framework for cross-border data transfers with ASEAN countries which consists of a set of contractual terms and conditions that parties may adopt in full or adapt for use in binding legal agreements for cross-border transfer of personal data. The MCCs are organized into two modules for controller-to-processor transfers and controller-to-controller transfers, respectively. The MCCs are also intended to be baseline in nature, and businesses are encouraged to check if the individual ASEAN Member States have provided further guidance or templates.

APEC CBPR and PRP Systems

Though all major SEA jurisdictions are members of the APEC, only the Philippines and Singapore participate in the APEC CBPR and PRP systems, and only Singapore has fully operationalized the systems within its data protection

law. Since 2019, Singapore's Infocomm Media Development Authority (IMDA) has been responsible for issuing CBPR certifications in Singapore. Further, in 2020, Singapore amended its Personal Data Protection Regulations to specify that transfers of personal data to recipients who are located outside Singapore but certified under the APEC CBPR or PRP would be deemed to satisfy the requirements of Singapore's data protection law.

Global CBPR Forum

In 2022, the Philippines and Singapore announced their participation in the Global CBPR Forum. Most recently, in April 2023, Singapore's IMDA was appointed Deputy Chair of the Forum, and the Philippines' National Privacy Commission was appointed to head the Forum's Communications and Stakeholder Engagement Committee.

Indonesia

Indonesia's Personal Data Protection Law (PDPL) was enacted on October 17, 2022, and was Indonesia's first comprehensive personal data protection law.

The PDPL provides data controllers or processors with a two-year transition period from its date of enactment to ensure compliance with its provisions. During this transition period, non-compliance with the PDPL will not result in any legal consequences (including administrative sanctions) for the controllers or processors.

The enactment of the PDPL brought much-needed clarity to a previously legal fragmented landscape where provisions on personal data protection were distributed across more than 30 different laws and regulations.

Article 56 of the PDPL sets out the requirements for transferring personal data out of Indonesia. This Article establishes a tiered structure consisting of three separate legal bases for transferring personal data out of Indonesia. In particular, data controllers must either:

- Ensure the destination has an equal or greater level of personal data protection compared to that mandated by the PDPL;
- Put in place adequate and binding safeguards; or
- Obtain consent for the data transfer.

Further details on each of these legal bases are provided below.

Equal or Greater Level of Personal Data Protection

In the first instance, a data controller or processor that wishes to transfer personal data out of the Republic of Indonesia must ensure that the governing law of the jurisdiction where the recipient is domiciled provides a level of personal data protection that is equal to, or greater than, that provided by the PDPL.

This provision appears similar to the adequacy basis in the GDPR. However, unlike the GDPR, the PDPL does not specify a mechanism or other criteria for determining whether another legal system provides an equal or greater level of protection of personal data than that provided by the PDPL.

Article 56(5) specifies that further provisions on the transfer of personal data will be specified in a forthcoming government regulation. It is expected that such government regulation will provide more clarity on the PDPL's mechanism for assessing the 'adequacy' of personal data protection provided by other legal systems. In this regard, Indonesia's Ministry of Communication and Information Technology has announced that it plans to release detailed implementing regulations for the PDPL by the end of 2023. However, the Ministry has not yet stated publicly whether these regulations will address cross-border data transfers.

Adequate and Binding Safeguards

If a personal data controller is unable to ensure an equal or greater level of personal data protection, the controller must put in place adequate and binding safeguards. The scope of this obligation is unclear as the PDPL does not specify criteria for what constitutes "adequate and binding safeguards."

It is possible, but still unclear, that such safeguards may involve the inclusion of data protection obligations in contracts (such as the ASEAN MCCs) or binding corporate rules in the context of intra-group companies transfer with the recipient of the personal data transferred. Again, this may be clarified in forthcoming government regulation, if enacted.

Consent

Finally, if a controller is unable to (a) ensure an equal or greater level of personal data protection, and/or (b) put in place adequate and binding safeguards, the controller must obtain the data subject's consent to the cross-border transfer of their personal data.

This is the basis that businesses are most likely to rely on until subsidiary regulations are issued, as the PDPL does specify requirements for valid consent for cross-border data transfers. Specifically, when relying on consent for transferring personal data out of Indonesia, controllers must take into account the requirements set forth under Articles 22-26 of the PDPL, which are as follows:

- Consent must be express, meaning that it must be in writing or recorded;
- A consent request (**request**) must be separate from other terms and conditions;
- The request must be easily understood and accessible;
- The request must use clear and plain language (including in Indonesian language);
- The request must be preceded by a privacy notice consisting of, among others, the lawful basis relied on, purposes, types of personal data processed, retention, and the data subject's rights;
- The controller must keep evidence of consent; and
- If the personal data transferred involves personal data of children and disabled people, their parents or legal guardians' consent must be obtained.

Penalties

Non-compliance with the PDPL's cross-border data transfer requirements may result in the imposition of one or more of the following administrative sanctions:

- Issuance of a written warning by the data protection authority;
- Temporary suspension of personal data processing;
- Deletion or destruction of personal data; and/or
- Administrative fines of up to 2% of the annual revenue or income from the violation.

Sectoral Requirements

In addition to the cross-border data transfer rules under the PDPL, businesses intending to carry out such data transfer must be aware of the same rules set forth under various sectors and subject matter-specific laws and regulations. For example, organizations engaging in the digital sector must adhere to the cross-border data transfer rules under, among others, Government Regulation 71/2019 on Provision of Electronic Systems and Transactions (GR 71/2019) and the Ministry of Communication and Information Technology ("**MOCIT**") Regulation No. 20 of 2016 on Personal Data Protection in Electronic System (MOCIT Regulation 20/2016).

Both the GR 72/2019 and the MOCIT Regulation 20/2016 will continue to be applicable as long as the rules therein do not contradict with the PDPL.

Under the MOCIT Regulation 20/2016, any cross-border personal data transfer from Indonesia must be reported to the MOCIT. This reporting is typically done using a standard template, which must be sent to the MOCIT's designated email address and contain information such as:

- The destination of the transfer;
- The name of the recipient;
- The date on which the cross-border personal data transfer will be conducted; and
- The purpose of the cross-border personal data transfer.

Additionally, a separate report must also be filed with the MOCIT after the completion of the cross-border personal data transfer, providing details of the cross-border personal data transfer's results.

Thailand

Thailand's Personal Data Protection Act (PDPA) provides the main requirements under Thai law relating to the collection, use, and disclosure of personal data. Though the PDPA was fully enacted in May 2019, it was only intended to take effect on May 27, 2020. The effective date was subsequently postponed to 2022 by the Thai government, due to the COVID-19 pandemic.

Sections 28 and 29 of the PDPA govern cross-border transfers of personal data and provide nine legal bases for transferring personal data out of Thailand:

- Adequate standard of personal data protection;
- Certified binding corporate rules (BCRs);
- Adoption of safeguards;
- Legal compliance;

- Consent;
- Necessity for execution or performance of a contract with the data subject;
- Compliance with a contract in the interests of the data subject;
- Preventing danger to life or health; and
- Necessity for public interest activities.

Several important developments in relation to the PDPA took place in 2022. In January 2022, the Thai government officially appointed the chairperson and members of Thailand's newly constituted Personal Data Protection Commission (PDPC), and in February 2022, the PDPC held its first meeting. In June 2022, the PDPA entered into effect, and the PDPC issued several subordinate regulations and guidelines expanding on the PDPA's requirements.

To date, the PDPC has not issued any binding regulations on cross-border data flows. However, in late September 2022, the PDPC released a "Draft Notification on Rules and Principles for Appropriate Personal Data Protection for International Data Transfers under the PDPA" (Draft Notification), together with an unofficial English translation, for public consultation. If enacted in its current form, the Draft Notification would:

- Provide detailed definitions for several important terms in the PDPA and
- Clarify the requirements for relying on the "certified BCRs" and "adoption of safeguards" based under Section 29 of the PDPA.

Public consultation on the Draft Notification concluded in late October 2022, and it remains to be seen how the PDPC will develop the Draft Notification based on the feedback received.

Adequate Standard of Personal Data Protection

Under Section 28 of the PDPA, transfers of personal data out of Thailand are permitted if:

- (1) The destination jurisdiction, or (2) the international organization (IO) that receives the data has an "adequate standard of personal data protection;" and
- The controller complies with rules prescribed by the PDPC (note: to date, the PDPC has not issued any such rules).

Section 28 of the PDPA provides a mechanism for the PDPC to review and make a determination as to whether a jurisdiction or IO has an "adequate standard of data protection." This system appears similar to the adequacy mechanism in the GDPR.

However, unlike the GDPR mechanism, Section 28 of the PDPA appears to only become operative if there is a "problem" with the adequacy of the standard of personal data protection in a specific jurisdiction or IO. In such a case, Section 28 of the PDPA provides that the problem should be submitted to the PDPC for determination. The PDPC's determinations are also subject to review if there is new evidence to suggest that the jurisdiction or IO has developed an "adequate standard of data protection."

To date, the PDPC has not issued any such "adequacy" decisions. The Draft Notification also did not provide details on how the PDPC would assess a jurisdiction's level of data protection.

Certified BCRs

Section 29(1) of the PDPA provides an exception to the default adequacy rule in Section 28 of the PDPA where:

- A data controller or processor in Thailand has put in place a personal data protection policy governing the transfer of personal data to a related controller or processor (such as another entity in the same corporate group) in another jurisdiction; and
- The policy has been reviewed and certified by the PDPC.

If enacted in its current form, Chapter 1 of the Draft Notification would provide high-level guidance on the PDPC's criteria for reviewing and verifying BCRs. Minimally, the policy would have to comply with the requirements of the PDPA and its subordinate regulations and would have to be legally binding on, and enforceable, against, all relevant entities and their employees.

Adoption of Safeguards

Section 29(3) of the PDPA further provides that in the absence of an adequacy decision under Section 28 of the PDPA or a certified personal data protection policy under Section 29 of the PDPA, a data controller or processor may transfer personal data out of Thailand if the controller or processor implements suitable protection measures which enable the enforcement of the data subject's rights, including effective legal remedial measures according to the rules and methods prescribed by the PDPC.

If enacted in its current form, Chapter 2 of the Draft Notification would provide guidance on which safeguards the PDPC would recognize as providing appropriate levels of protection for personal data transferred out of Thailand. These would include standard contractual clauses (provided in Appendices A and B to the Draft Notification), code of conduct, and certifications, provided that these measures meet certain criteria set out in the draft Notification.

Consent

Section 28(2) of the PDPA provides that a data controller or processor does not need to comply with the default adequacy requirement where:

- The controller or processor informs the data subject that their personal data will not be protected to the adequate standard after the transfer; and
- The data subject consents to the cross-border transfer of their personal data.

Others

- **Legal Compliance:** Section 28(1) of the PDPA provides that a data controller or processor does not need to comply with the default adequacy requirement where the cross-border transfer of personal data is for compliance with the law.

- **Necessity for Execution or Performance of a Contract with the Data Subject:** Section 28(3) of the PDPA provides that a data controller or processor does not need to comply with the default adequacy requirement where the cross-border transfer of personal data is 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.
- **Compliance with a Contract in the Interests of the Data Subject:** Section 28(4) of the PDPA provides that a data controller or processor does not need to comply with the default adequacy requirement where the cross-border transfer of personal data is for compliance with a contract between the controller and another person for the interests of the data subject.
- **Preventing a Danger to Life or Health:** Section 28(5) of the PDPA provides that a data controller or processor does not need to comply with the default adequacy requirement where the cross-border transfer of personal data is to prevent or suppress a danger to the life, body, or health of the data subject or another person when the data subject is incapable of giving the consent at such time.
- **Necessity for Public Interest Activities:** Section 28(5) of the PDPA provides that a data controller or processor does not need to comply with the default adequacy requirement where the cross-border transfer of personal data is necessary for carrying out the activities in relation to substantial public interest.

Penalties

Failure to comply with the PDPA's requirements for cross-border transfer of personal data is punishable with a fine of up to 3 million THB (approximately $87,000 USD).

If sensitive personal data is transferred out of Thailand in non-compliance with the PDPA's requirements, the fine increases to 5 million THB (approximately $144,500 USD).

Additionally, if the non-compliant transfer of sensitive personal data is likely to cause a person to suffer any damage (including reputational damage) or expose the person to scorn, hatred, or humiliation, the controller may be punished with up to six months imprisonment and/or a fine of up to 500,000 THB (approximately $14,400 USD).

If sensitive personal data is transferred out of Thailand to unlawfully benefit any person may be punished with up to a year's imprisonment and/or a fine of up to 1 million THB (approximately $28,800 USD).

Vietnam

On April 17, 2023, Vietnam enacted the long-awaited Decree No. 13/2023/ND-CP on personal data protection (PDPD), the country's first comprehensive legal instrument governing the protection of personal data. The PDPD took full effect on July 1, 2023, and applies to the following (collectively, "regulated entities"):

- Personal data controllers;
- Personal data processors;
- "Personal data controllers and processors" (organizations or individuals that function as both controllers and processors); and

- "Third parties" (any other organization or individual authorized to process personal data).

The PDPD is the first step in a broader legislative effort to govern the protection of personal data in Vietnam as Vietnam's Prime Minister has announced that the Vietnamese government plans to enact a more comprehensive law on personal data protection by 2024. Though the PDPD takes the form of a "decree" – a form of executive order which ranks below a "law" in Vietnam's legislative hierarchy – it is legally binding on all persons and organizations and sets out detailed obligations in relation to their processing of personal data.

Article 25 of the PDPD governs cross-border transfers of personal data, including the transfer of Vietnamese citizens' personal data out of Vietnam and outsourcing of the processing of Vietnamese citizens' personal data to a location outside of Vietnam.

This Article provides only a single procedure for legally transferring personal data out of Vietnam.

This procedure is closer to the security assessment mechanism in China's data protection framework than to any of the legal bases for transferring personal data under other data protection laws internationally, such as the GDPR. However, unlike China's security assessment mechanism, the PDP's procedure is mandatory for all entities covered by the PDPD, not just entities which operate critical infrastructure or process large volumes of personal data.

Data Transfer Assessment

In order to transfer personal data out of Vietnam, regulated entities must within 60 days from the date of processing the personal data:

- Conduct a "data transfer assessment" (DTA); and
- Submit a copy of the DTA, together with a prescribed form, to the Cybersecurity and High-Tech Crime Prevention Department (known as "A05") of Vietnam's Ministry of Public Security (MPS) – the authority responsible for administering the PDPD.

The DTA must contain the following information:

- Information and contact details of the transferor and receiver of the personal data of Vietnamese citizens;
- The full name and contact details of the organization and/or individual that is in charge of the transferor;
- Descriptions and explanations of the purposes for the transfer;
- Descriptions and clarification of the type of personal data to be transferred;
- Description and specification of compliance with the PDPD's data protection requirements, including details implementation of measures for safeguarding personal data;
- Assessment of the impact of personal data processing, the potential consequences and damage, and measures to reduce or eliminate such risk or harm;
- Details of the consent of the data subject given with a clear understanding of the feedback mechanism and complaint procedures available in the event of incidents or requests; and

- A binding contract between the transferor and the recipient specifying the responsibilities of the parties involved regarding the personal data processing.

Note that although Article 25 of the PDPD requires the DTA to include a copy of a binding contract, the PDPD does not require the agreement to take any specific form or contain any specific language beyond specifying the parties' responsibilities regarding the processing of personal data. It is therefore possible that an agreement based on the ASEAN MCCs would satisfy this requirement.

Under Article 25.7 of the PDPD, on receiving the DTA, the MPS may request further information from the entity or instruct the entity to cease the cross-border transfer of personal data if:
- The data is used for activities that violate Vietnam's interests and national security;
- The entity fails to complete or update the dossier of impact assessment; or
- The personal data of Vietnamese citizens is lost or leaked.

In addition to the above requirements, regulated entities must also make a copy of the DTA available for inspection by the MPS at any time and notify A05 after the cross-border transfer has successfully taken place. The cross-border transfer may also be subject to annual inspection by the MPS.

Consent

Consent is not an independent legal basis for transferring personal data out of Vietnam under the PDPD. However, the PDPD appears to require regulated entities to obtain consent for cross-border data transfers, in addition to requiring such entities to undertake a DTA and file it with the MPS.

Notably, Article 25 of the PDPD requires regulated entities to include details of the data subject's consent to the cross-border data transfer. This requirement may be read with Article 11 of the PDPD, which requires regulated entities to obtain consent for all processing of personal data, including transfers, unless an exception applies.

Under Article 11 of the PDPD, consent is only valid if it is voluntary and if the data subject has been informed of:
- The specific types of personal data being processed;
- The purposes of processing;
- The organizations or individuals involved in the processing (such as the recipient of a cross-border data transfer), and
- The data subject's rights and obligations under the PDPD.

Article 17 of the PDPD outlines several exceptions to the consent requirement, which are similar to necessity bases under other data protection laws internationally. These include:
- Emergencies threatening the life and health of persons;
- National and public interest concerns;
- The operation of state agencies;
- Performance of a contract; and

- Where personal data has legally been made public.

Given the express consent requirement in Article 25 of the PDPD, it is unclear if these exceptions apply in the context of cross-border data transfers.

Penalties

The PDPD does not prescribe specific penalties for failing to comply with its cross-border data transfer requirements and instead, contains a general provision that non-compliance may be subject to disciplinary action, administrative penalties, or criminal prosecution.

It is likely that Vietnamese authorities will issue regulations outlining penalties and other sanctions for noncompliance with the PDPD in the future.

In June 2023, following the issuance of the PDPD, the MPS released the latest in a series of draft "Regulations on Sanctioning Administrative Violations in the Field of Cybersecurity" (Draft Penalty Decree) that, if enacted, would specify administrative sanctions for violations of the PDPD, including cross-border data transfer requirements.

Although the Draft Penalty Decree has not yet been enacted, it notably sought to introduce penalties from 80 million VND (approximately 3,400 USD) to 100 million VND (approximately $4,200 USD) for failing to comply with conditions for transferring personal data out of Vietnam provided in the PDPD, such as:

- Failure to create or retain the DTA for the transfer of personal data abroad from the moment the processing of personal data begins.
- Failure to submit an original copy of the DTA to A05 within 60 days from the date of processing personal data.
- Failure to provide written notification to A05 regarding the data transfer and contact details of the responsible organization or individual after the successful data transfer.
- Failure to comply with the requirements for amending and completing the DTA for the transfer of personal data abroad as requested by A05.
- Failure to comply with the requirements for inspecting the transfer of personal data abroad as requested by A05.

Under the Draft Penalty Decree, twice the penalty amount would apply if the violation results in the unauthorized disclosure or loss of personal data of 100,000-1,000,000 Vietnamese citizens. Five times the penalty amount would apply if the violation results in the unauthorized disclosure or loss of personal data of 1,000,000-5,000,000 Vietnamese citizens. If the violation concerns the personal data of over 5,000,000 Vietnamese citizens, a fine ranging from 3% to 5% of the offender's total revenue for the preceding fiscal year in Vietnam would apply.

The Draft Penalty Decree also would have prescribed other sanctions, including:

- The temporary suspension of business licenses for a period of 1 to 3 months;
- Seizure of assets and personal data processing equipment, and
- Deportation of foreign individuals;

- Permanent deletion or erasure of personal data beyond recovery;
- Restitution or surrender of any illicit gains derived from the violations, and
- Public apology through public media channels for the committed violations.

Data Localization

Under Vietnam's Law No. 24/2018/QH14 on Cybersecurity and its implementing regulation, Decree 53/2022/ND-CP (Decree 53), certain service providers must store the following kinds of personal data within Vietnam:

- Personal data of service users in Vietnam;
- Data generated by users in Vietnam, including user account names, service usage duration, credit card information, email addresses, login and logout IP addresses, phone numbers associated with the account, or other related data; and
- Data on relationships of users in Vietnam, including friends, groups, or interactions that the user connects or engages in

(collectively, "prescribed data")

This obligation applies to service providers that:

- Provide services over telecommunications networks, the Internet, and other value-added services in cyberspace within Vietnam; and
- Engage in the collection, mining, analysis, and processing of prescribed data.

Vietnamese companies that meet the aforementioned conditions would have to comply with data residency requirements outlined under Decree 53, since it came into force in October 2022.

For foreign companies, pursuant to Article 26.3 of Decree 53, these obligations extend to companies established or registered under foreign law (foreign companies) only if the following conditions are met:

- The foreign company conducts business activities in Vietnam in one of the 10 following sectors:
    - telecommunications services;
    - storage and sharing of data in cyberspace;
    - provision of national or international domain names to users in Vietnam;
    - e-commerce;
    - online payment services;
    - payment intermediaries;
    - connectivity services through cyberspace;
    - social networks and social media;
    - online gaming;
    - provision, management, or operation of other information services in cyberspace, such as messaging, voice calls, video calls, email, and online chat.

- A05 has:

- notified the foreign company that a service provided by the company has been utilized to engage in activities that violate Vietnam's cybersecurity laws and
- issued a written request for the company to respond to the violation.

- The foreign company has failed to comply fully with A05's request or has otherwise interfered with or nullified cybersecurity protection measures implemented by A05.

Under Article 27 of Decree 53, the foreign company must store the prescribed data within Vietnam for the duration of the written request from A05. Furthermore, it is explicitly mandated that "the minimum storage period is 24 months." While it is unclear whether this minimum storage requirement applies to all domestic and foreign entities, one plausible interpretation is that, given its immediate placement after the data storage requirement upon request, it specifically applies to foreign companies.

An earlier draft of the Draft Penalty Decree proposed administrative sanctions for violations of data localization requirements, including penalties ranging from 80 million VND (approximately $3,400 USD) to 100 million VND (approximately $4,200 USD) for individual violations, along with supplementary measures such as deportation, temporary suspension of business license, and the forfeiture of any unlawfully acquired benefits arising from these violations.

Annex 3: Northeast Asia

While Northeast Asia's data protection landscape is well established, both **Japan** and **South Korea** regularly review and amend their data protection laws. Notably, the most recent rounds of amendments to data protection laws in both **Japan** (2021 and 2022) and **South Korea** (2023) directly addressed provisions on cross-border data transfers. These amendments are discussed in further detail below.

Both jurisdictions are also active in international initiatives to promote interoperability between national data protection laws and facilitate cross-border data flows.

APEC CBPR and PRP Systems
Both Japan and South Korea currently participate in the APEC CBPR system, and both jurisdictions have operationalized the systems within their respective national laws. Since 2016, JIPDEC (known as the "Japan Information Processing and Development Center" until 2011) has been responsible for issuing CBPR certifications in Japan. Since 2019, the Korea Internet and Security Agency has been responsible for issuing CBPR certifications in South Korea.

Global CBPR Forum
In 2022, Japan and South Korea announced their participation in the Global CBPR Forum. In April 2023, Japan's Ministry of Economy, Trade, and Industry (METI) was appointed to chair the Forum's Membership Committee.

EU Adequacy
Both Japan and South Korea have mutual adequacy decisions with the EU. The European Commission published its final adequacy decisions for Japan's private-sector privacy law In January 2019 and for South Korea's privacy law in December 2021. These decisions determine that the level of personal data protection in Japan and South Korea jurisdictions is "essentially equivalent" to that under the GDPR and permits transfers of European personal data to these jurisdictions without the need for implementation of any additional safeguards, such as SCCs or BCRs.

Data Free Flow with Trust (DFFT)
In recent years, Japan's efforts to promote the concept of "Data Free Flow with Trust" (DFFT) – a broad vision for the free flow of data (including personal data) across borders while ensuring consumer and business trust in privacy, security, and intellectual property rights – have been gaining momentum in international fora.

The concept of DFFT was introduced in a speech by former Japanese Prime Minister Shinzo Abe during the World Economic Forum (WEF) Annual Meeting in Davos in January 2019. The concept has been restated and further developed in multiple international fora, including:

- The G20 Summits in Osaka (June 2019) and Riyadh (November 2020);
- The G7, which adopted a roadmap for cooperation on DFFT (April 2021), and action plan for promoting DFFT (May 2022); and

- The WEF in a 2020 whitepaper, and
- The OECD in whitepapers released in 2022 and 2023.

While high-level support for the concept has been growing in international fora, there have also been long-standing questions as to how to operationalize it. Throughout 2023, the concept has begun to take shape with support from multiple ministries and agencies within the Japanese government – including Japan's Digital Transformation Agency, METI, and Ministry for Internal Affairs and Communication (MIC) – using Japan's G7 presidency as a platform to garner greater support for the initiative.

Additionally, promotion of DFFT is now a key strategic objective in the 2023 Global Strategy of Japan's Personal Information Protection Commission (PPC), which links the concept to the PPC's work to promote international corporate certification systems, such as the emergent Global CBPR Forum, and introduce global model contract clauses.

A major milestone is the G7 Ministerial Declaration adopted by digital ministers from the G7 economies, together with the DTA, METI, and MIC, in April 2023. Annex 1 of the Declaration outlines the G7's vision for operationalizing DFFT.

Notably, the Declaration endorsed the establishment of an Institutional Arrangement for Partnership (IAP) to "operationalize DFFT through principles-based, solutions-oriented, evidence-based, multi-stakeholder and cross-sectoral cooperation." The IAP is expected to bring together stakeholders and the broader community of data governance experts to consider several issues, including:

- Development of compatible policies, tools, and practices for enabling data flows in full compliance with existing regulatory requirements regarding data;
- Key impediments and challenges to DFFT;
- Technological developments that relate to DFFT such as privacy enhancing technologies (PETs); and
- Legal practices enabling DFFT, such as model contractual clauses, certification mechanisms, and international privacy frameworks.

Most recently, the PPC added promotion of DFFT to the agenda for the 3rd annual G7 Data Protection and Privacy Authorities Roundtable, held in Tokyo from June 20 to 21, 2023.

Japan

Japan has seen several developments in relation to cross-border data transfers in the last three years, including amending relevant provisions of its main data protection law, the Act on Protection of Personal Information (APPI), and promoting an initiative called "Data Free Flow With Trust" (DFFT) in international fora, including most recently, the Group of Seven (G7) which Japan is hosting in 2023.

Cross-Border Data Transfers under the APPI

Article 28 of the APPI sets out the main requirements under Japanese law for transferring personal information (PI) out of Japan.

A "business operator handling PI" (Operator) (this term covers both controllers and processors as defined in the GDPR) must obtain the data subject's consent to transfer PI out of Japan unless one of the following conditions applies:

- **Adequacy Decision:** Japan's data protection authority, the Personal Information Protection Commission (PPC), has recognized that the destination jurisdiction has established a system that protects individuals' rights and interests in their PI to an equivalent standard to the APPI. To date, the PPC has recognized the EU and the UK GDPRs as systems that provide an equivalent standard of personal data protection to Japan's APPI.
- **Equivalent Measures**: The overseas recipient of the PI has established a system that conforms to standards prescribed by the PPC as equivalent to those in the APPI. The PPC has recognized the APEC CBPR system as providing "equivalent measures" for the purpose of Article 28 of the APPI.
- **Legal Compliance:** The cross-border transfer is based on other laws or regulations.
- **Necessity to Protect Vital Interests**: The cross-border transfer is necessary to protect the life, health, or property of an individual, and it is difficult to obtain that individual's consent.
- **Necessity for Public Health etc.**: The cross-border transfer is necessary to improve public health or promote healthy development of children, and it is difficult to obtain individual consent.
- **Necessity to Cooperate with Authorities:** The cross-border transfer is necessary for cooperation with a government entity, or person entrusted with performing functions prescribed by laws and regulations, and obtaining individual consent would likely interfere with the performance of those functions.
- **Academic Research Exceptions:** See the section on "2021 amendments" below.

The APPI was substantially amended in 2020 and 2021. Both sets of amendments took effect in April 2022.

2020 amendments: Clarifying and disclosure and due diligence requirements for cross-border data transfers

The 2020 amendments and accompanying updates to the PPC's cross-border data transfer guidelines (PPC Guidelines) clarified the scope of the APPI's "equivalent measures" and "consent" mechanism for cross-border transfers.

Following the amendments, any Operator that seeks to rely on the APPI's "**equivalent measures**" mechanism to transfer PI to an overseas recipient must:

- Take "necessary action" to ensure that the overseas recipient continuously implements the "equivalent measures;" and
- On request by a data subject, provide the data subject with information on the actions taken by the Operator to ensure that the overseas recipient continuously implements such measures.

Necessary Action

The PPC Guidelines interpret "necessary action" as requiring the transferring Operator to:

- Periodically check the implementation status and content of the APPI-equivalent measures by the recipient third party, and use an "appropriate and reasonable method" to identify any foreign laws which might impact such implementation;
- Take necessary and appropriate actions to remedy any obstacles that are found; and
- Suspend all PI transfer to the overseas recipient, if it becomes difficult for the recipient to continuously implement APPI-equivalent measures.

The PPC Guidelines also require Operators, who receive an information request from a data subject regarding the actions taken to ensure that the overseas recipient continuously implements "equivalent measures," to provide the data subject following information without delay:

- The manner by which the overseas recipient has established APPI-equivalent measures (e.g., a data processing agreement or memorandum of understanding, or in the case of inter-group transfers, a privacy policy);
- Details of the APPI-equivalent measures implemented by the overseas recipient;
- The frequency and method by which the transferring Operator checks such implementation;
- The name of the recipient country;
- Whether any foreign laws may affect the implementation of the APPI-equivalent measures, and a detailed overview of such laws;
- Whether any obstacles to implementation exist, and a detailed overview of such obstacles; and
- The measures taken by the transferring Operator upon a finding of such obstacles.

The Operator may refuse to disclose certain information but only if providing the information would be likely to 'significantly hinder' the Operator's business operations.

Consent

Additionally, operators seeking to rely on consent must – in addition to complying with pre-existing notification obligations – inform the data subject in advance of:

- The foreign jurisdiction to which their PI will be transferred,
- The levels of PI protection provided by the destination jurisdiction (this information must be obtained using appropriate and reasonable methods); and
- The measures that the recipient takes for the protection of personal information.

If the Operator does not provide this information to the data subject, the data subject's consent will not be considered valid, and the transfer will not be in compliance with the APPI.

2021 amendments: New transfer mechanisms for academic institutions

Prior to the 2021 amendments, academic research institutions were uniformly exempted from obligations under the APPI when handling personal information for academic research purposes.

The 2021 amendments removed this uniform exemption and replaced it with more specific exceptions to individual obligations under the APPI, including – notably – the obligation to obtain consent for cross-border data transfers.

Following the 2021 amendments, Operators that are, or are equivalent to, academic institutions may transfer PI out of Japan without obtaining an individual's consent to the transfer, if the transfer is:

- Necessary for performance of its functions prescribed by law, and obtaining individual consent would likely interfere with the performance of those functions.
- Unavoidably necessary for publication of academic research or teaching, and there is no risk that the transfer would unjustly infringe on the individual's rights and interests;
- Necessary for academic research purposes, and there is no risk that the transfer would unjustly infringe on the individual's rights and interests.

South Korea

South Korea's Personal Information Protection Act (PIPA), which was enacted in 2011, is South Korea's main data protection law and together with its implementing regulations, governs the processing of PI by PI controllers in South Korea.

In March 2023, South Korea's government enacted major amendments to the PIPA (note: link is in Korean). These amendments, which will take effect on September 15, 2023, will add a new section (Section 4) to the PIPA which will unify its existing provisions on cross-border transfers of PI and introduce two new legal bases: **certification** and **adequacy**. However, notably, the amendment bill does not refer to SCCs or BCRs.

In May 2023, South Korea's government also proposed amendments to the Enforcement Decree to the PIPA (Enforcement Decree), which will also take effect on September 15, 2023. These amendments provided further detail on how the new PIPA provisions will be implemented.

New Legal Bases

Once the amendments to the PIPA take effect in September 2023, the full list of legal bases from cross-border transfers of PI under the PIPA will be as follows:

- **Consent:** PI may be transferred out of South Korea if the PI controller obtains the data subject's consent to the transfer. Consent for cross-border transfers of PI must be obtained separately from consent for collection and use of the PI, and the data subject must be informed of certain prescribed matters, including:
    - the items of PI that will be transferred;
    - the destination jurisdiction;
    - the time and method of transfer;
    - the name of the recipient;
    - the purpose for the transfer;
    - the period in which the PI will be used and retained; and

    - the method and process for the data subject to refuse the transfer, and the effect of such refusal.
- **International Agreements:** PI may be transferred out of South Korea pursuant to special rules under treaties and other international agreements to which South Korea is a party.
- **Necessity for Execution and Performance of a Contract with the Data Subject:** PI may be transferred out of South Korea for the purpose of outsourcing the processing of that PI. In this case, the transferor must provide certain information to the data subject either through its privacy policy or via prescribed methods, such as email.
- **Certification**: PI may be transferred out of South Korea where the transferor has received certification, which will be designated by South Korea's Personal Information Protection Commission (PIPC).
- **Adequacy**: PI may be transferred out of South Korea where the PIPC has determined that the destination jurisdiction or international organization has a substantially equal level of data protection to that of the PIPA.

PIPC's Power to Suspend Cross-Border Data Transfers

The 2023 amendments also provide the PIPC with new power to order the suspension of cross-border transfers if:

- The transfer violates the PIPA's cross-border data transfer requirements; and
- The recipient of transferred PI or the country where personal information is transferred fails to properly protect the PI to a comparable standard to that under the PIPA, and such failure may cause, or has caused, significant harm to the data subject.

The amendments also provide that a PI controller may file an objection to the order within seven days of receiving it. The standard for the suspension order and the procedure for making such an objection will be specified in a forthcoming Presidential Decree.

Penalties

Under the 2023 amendments, non-compliance with the new PIPA's cross-border transfer requirements or a suspension order from the PIPC order may be subject to a penalty of up to 3% of the PI controller's total sales revenue or, where the controller has no sales or it is difficult to calculate the controllers' sales revenue, up to 2 billion KRW (approximately 1.5 million USD).

Creation of an Overseas Transfer Expert Committee

Notably, the 2023 amendments to the Enforcement Decree seek to create a new "**Overseas Transfer Expert Committee**" (OTEC) that will be responsible for advising the PIPC on matters relating to the new PIPA provisions on cross-border transfers of personal data, including:

- Reviewing proposals by the PIPC to establish a certification scheme for cross-border data transfers;
- Evaluating whether a destination jurisdiction or international organization offers a "substantially equivalent" level of data protection to that offered by the PIPA; and
- Whether to order suspension of cross-border data transfer.

In August 2023, the PIPC commenced a public consultation on a set of draft regulations, which would provide further detail on the composition of the OTEC and how the OTEC should perform the above functions.

Washington, DC | Brussels | Singapore | Tel Aviv

info@fpf.org

FPF.org