

# International Cooperation Project 2022 for Promoting Regulatory Reform

Research on trends in corporate certification  
in other countries related to data protection  
and cross-border data transfer

Research Report

February 2023



# Contents

<b>1</b>	<b>Position of This Project</b>	<b>P. 02 - 05</b>
	1.1 Background .....	P. 03
	1.2 Research Approach .....	P. 04 - 05
<b>2</b>	<b>Research related to Cross-Border Data Transfer</b>	<b>P. 06 - 109</b>
	2.1 Research Objectives and Summary .....	P. 07 - 14
	2.2 Details of the Results: Regulations/International Rules .....	P. 15 - 58
	2.3 Details of the Results: Cross-Border Data Transfer Tools .....	P. 59 - 84
	2.4 Details of the Results: Other Relevant Tools .....	P. 85 - 109
<b>3</b>	<b>Research on the Actual Utilization by Businesses</b>	<b>P. 110 - 138</b>
	3.1 Research Objectives and Approach .....	P. 111 - 115
	3.2 Summary of the Results .....	P. 116 - 121
	3.3 Details of the Results: Business Interviews .....	P. 122 - 138
<b>4</b>	<b>Summary of Research Results</b>	<b>P. 139 - 142</b>



# Agenda

- 1. Position of This Project
- 2. Research related to Cross-Border Data Transfer
- 3. Research on the Actual Utilization by Businesses
- 4. Summary of Research Results



# Background and Objectives



## Background/Objectives

### Background:

In the digital age, data is a source of added-value. The importance of extracting that value is increasing for business activities.

Related regulations that reflected ideas/stances about the economy and individual rights have been developed in the world since the 1990s.

From a practical perspective, there are a variety of tools (certifications, standards etc.) for cross-border data transfer. On the other hand, there are some moves toward rule integration such as CBPR.

### Objectives:

- Collect and analyze information that will serve for the operationalization and future improvement of the new Global CBPR forum
- Conduct a detailed survey of the data (not limited to personal data) certification schemes in each economy and region



## Research Plan

Conducted the followings based on previous studies<sup>1</sup>

- Organize the concept of regulations/tools for cross-border data transfer
- Detailed analysis of the contents of regulations/tools
- Identification of issues and business needs for existing tools/cross-border data transfer through interviews

1. [https://www.meti.go.jp/meti\\_lib/report/2021FY/000376.pdf](https://www.meti.go.jp/meti_lib/report/2021FY/000376.pdf), [https://www.meti.go.jp/shingikai/mono\\_info\\_service/data\\_ekkyo\\_iten/pdf/20220228\\_2.pdf](https://www.meti.go.jp/shingikai/mono_info_service/data_ekkyo_iten/pdf/20220228_2.pdf), [https://www.meti.go.jp/meti\\_lib/report/2021FY/000377.pdf](https://www.meti.go.jp/meti_lib/report/2021FY/000377.pdf), [https://www.ppc.go.jp/files/pdf/nichibeiou\\_ekkyouiten\\_report.pdf](https://www.ppc.go.jp/files/pdf/nichibeiou_ekkyouiten_report.pdf)



# Research Approach (1/2)

We created a list of regulations/tools for cross-border data transfer and held interviews to research actual activities

Research on  
Cross-Border  
Data Transfer



Create List of  
Target  
Regulations

Analyze and Compare Requirements

Create List of  
Target  
Tools

Analyze and Compare Requirements

Research on the  
Actual Utilization  
by Businesses



Hold Interviews for Businesses

Identify Needs and Pain  
Points

Summary of  
Research  
Results



Summarize Result

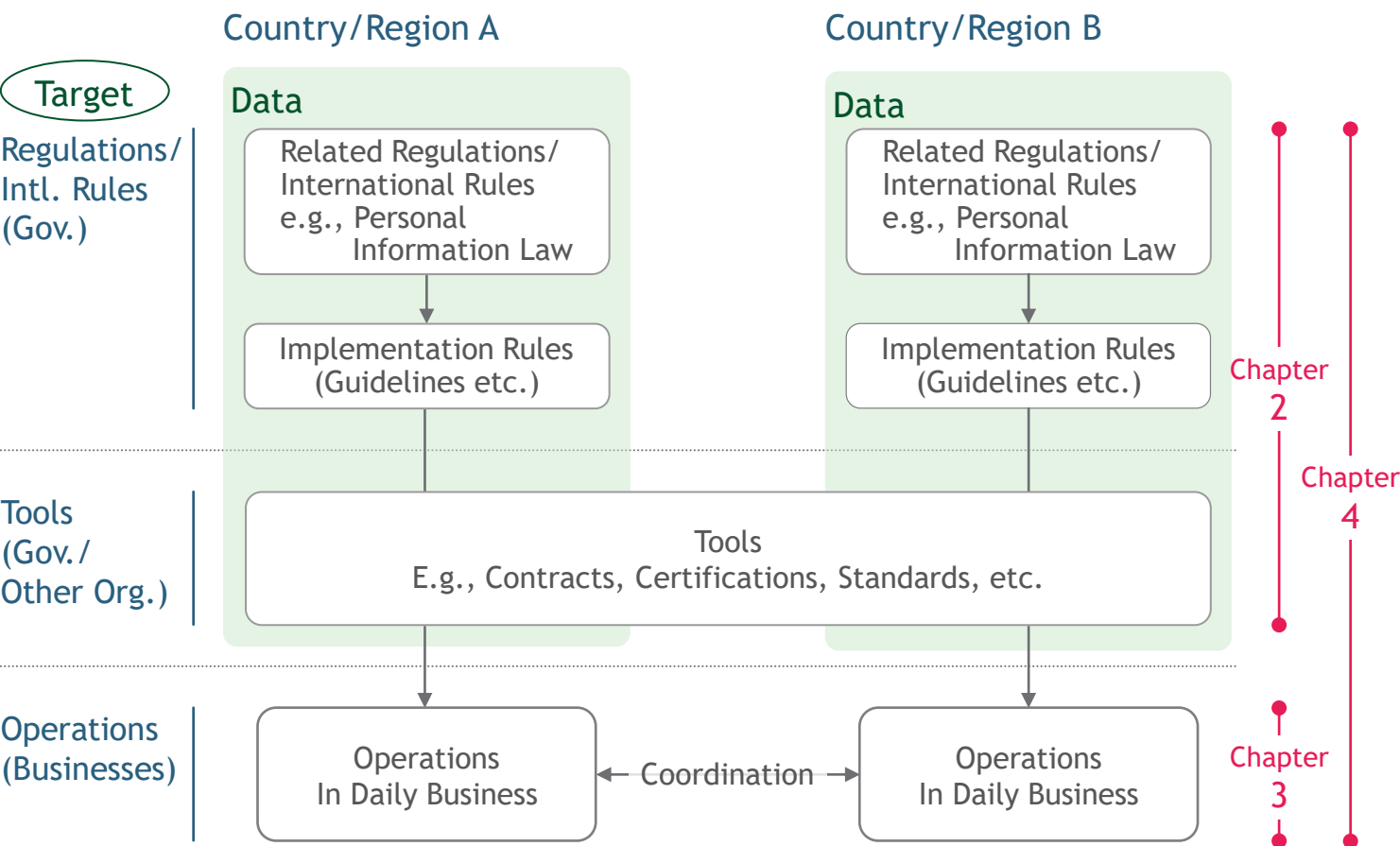


# Research Approach (2/2)

Organized the cross-border data transfer practices as follows, and researched highlighted regulations/tools

## Cross-Border Data Transfer Operations

Businesses conduct cross-border data transfer in their daily operations. To carry out transfers, operators implement relevant regulations and utilize tools.



### Approach

While the purpose of this study is to "collect and analyze data protection-related information", "data protection-related regulations" are put into practice in the flow shown on the left

Therefore, this survey will organize information based on the framework on the left.

Chapter 2  
Organize regulations/ international rules and tools

Chapter 3  
Survey actual status of cross-border data transfer operations of business operators

Chapter 4  
Summarize overall findings of survey and derive suggestions for consideration of new forum



# Agenda

1. Position of This Project
- 2. Research related to  
Cross-Border Data Transfer
3. Research on the Actual Utilization  
by Businesses
4. Summary of Research Results





## 2.1

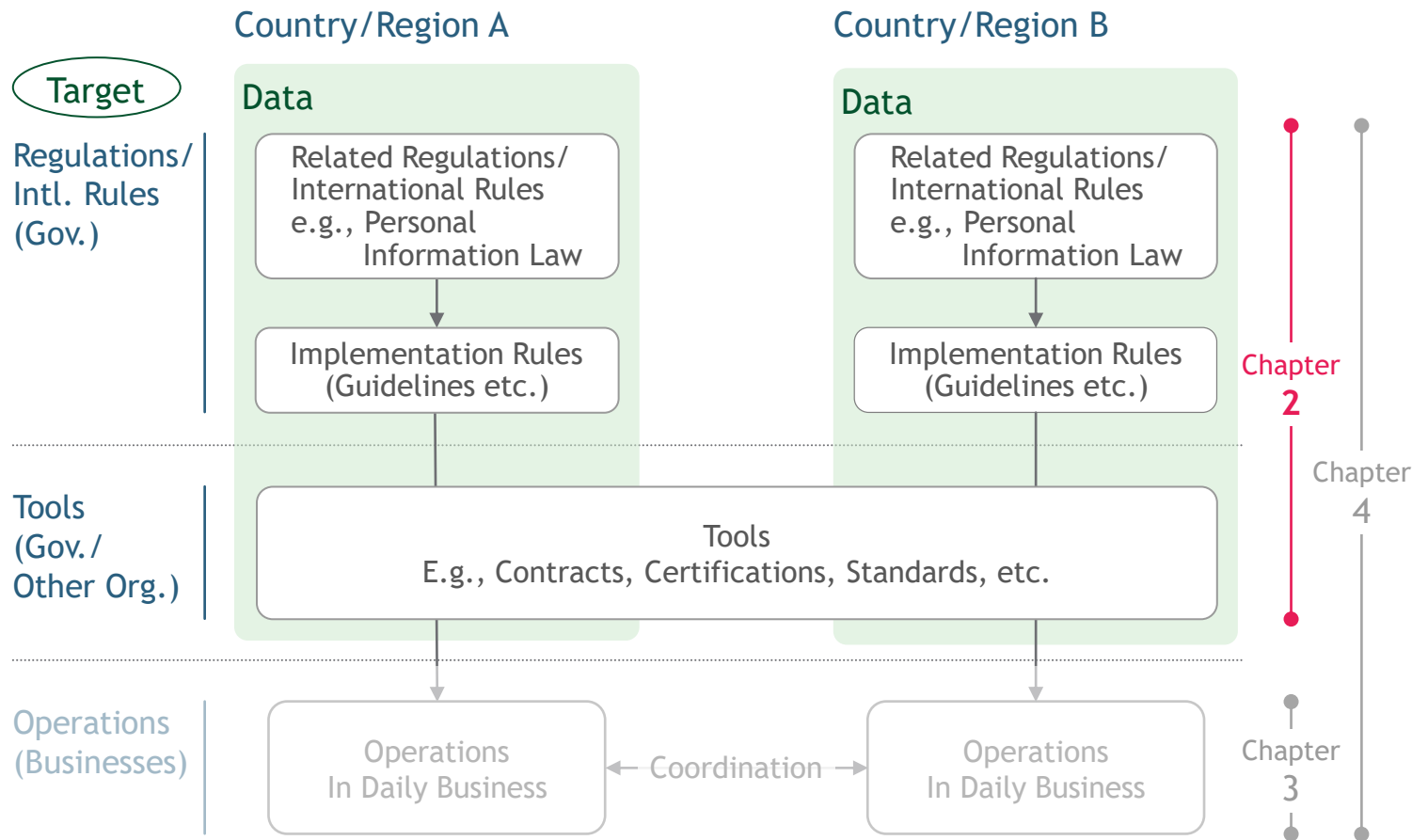
# Research Objectives and Summary



# Objectives of Chapter 2

## Cross-Border Data Transfer Operations

Businesses conduct cross-border data transfers in their daily operations. To carry out transfers, operators enforce the relevant regulations and utilize tools



## Objectives

- Provide overview of regulations and international rules
- Organize tools and their requirements
- Observe current international trends in cross-Border data transfer

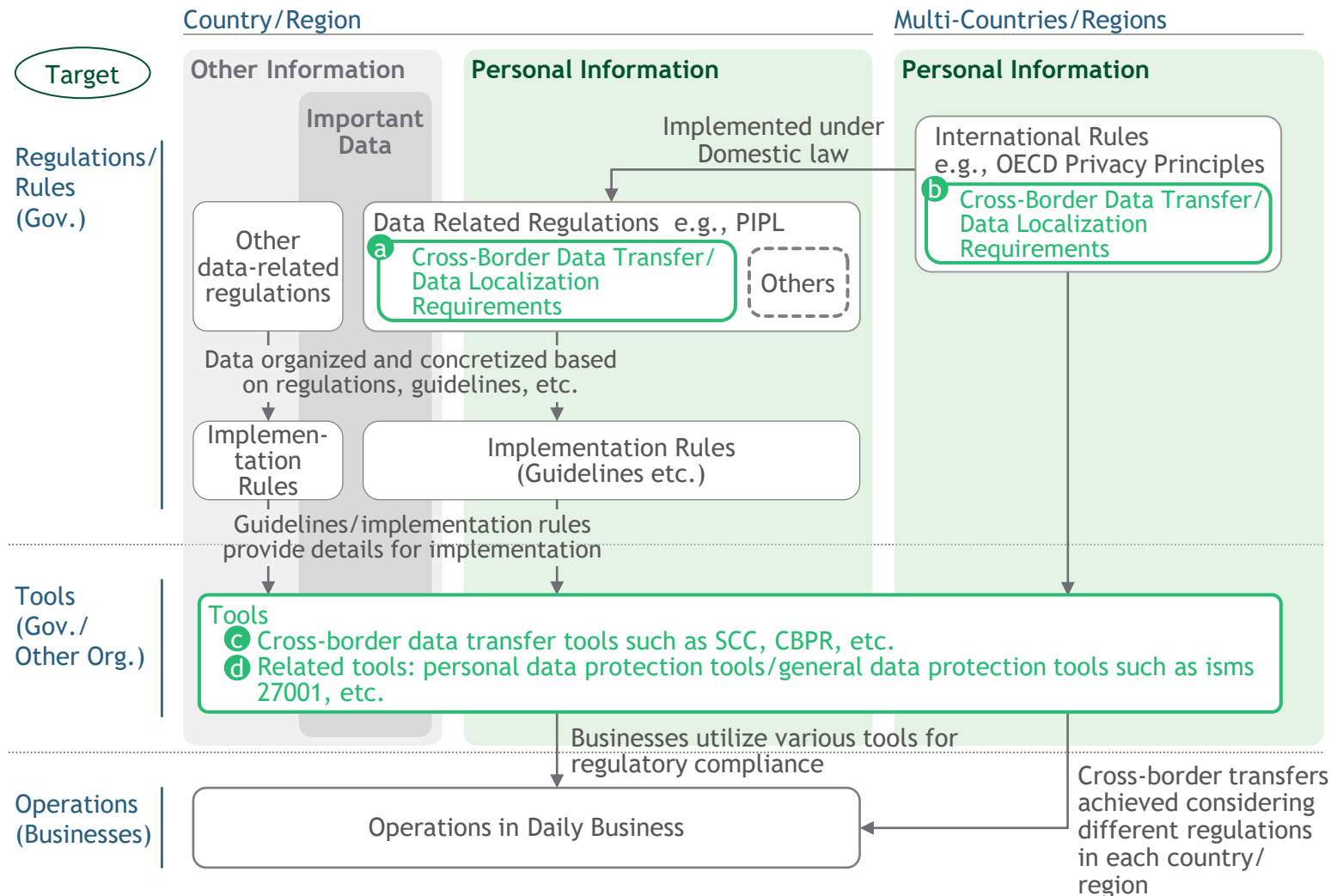
After this chapter, research the actual operations according to the result of this chapter.



# Approach of Chapter 2

In this study, we organized the concepts around cross-border data transfer as follows, and set the scope as **a** - **d**

## Cross-Border Data Transfer Operations



## Approach

The regulations/international rules and tools for cross-border data transfer can be organized in more detail as shown on the left.

Specifically, in most cases, data-related regulations, mainly privacy laws of each country/region, govern the cross-border data transfer. Regulations include those related to the cross-border transfer itself and localization regulations, which include national data storage obligations that affect such regulations. In addition, since regulations at the country/regional level are influenced by international rules, **the two cross-border transfer-related regulations and international rules are also included in this study.**

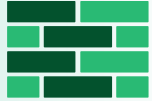
In light of the current globalization of cross-border data transfers, **22 countries/regions, including Japan, and relevant international organizations** were selected for the survey on regulations.

As for tools, in addition to tools related to cross-border transfers themselves, **relevant personal data protection tools and general data protection tools will also be investigated.**



# Summary of the Research on Regulations (1/3)

## Current Situation



The cross-border data transfer involves a number of systems: international rules, regulations, certifications, etc. **Businesses must take individual measures for data distribution, depending on their objectives and the distribution**

Although each system is independent, they interact with each other, **and a certain trend has emerged recently.**

- **International Rules:**  
The basis is OECD/APEC Privacy Principles. There are some little differences between each principles, **but generally same**
- **Regulations:**  
Each country/region is developing its own rules based on the international rules. Currently, there are 4 trends. In these trends, **the EU is leading the way and the adoption of GDPR-like regulations is increasing, especially in less developed countries**
- **Cross-Border Data Transfer Tools:**  
Various tools exist, mainly those regulated by the GDPR. **SCC/MCC** is becoming popular even in countries that do not have GDPR-type regulations (e.g., China), and **has been adopted by the largest number of countries as a cross-border data transfer tool**
- **General Data Protection Tools:**  
There are many certification systems based on domestic regulations. **Commonality in requirements and connections to cross-border transfer tools are being developed** to improve the convenience of personal data protection/data distribution

## Future Direction (Suggestion)



While there are various regulations and tools for cross-border data transfer, **there are some commonalities, and it is expected that connections and integration among these tools will be made on a global basis**

- In South Korea, there is an example of unification of systems due to the proliferation of data protection-related certifications
- Taiwan recommends connecting the general data protection certification (scope: domestic) and the global certification based on its own regulations to promote efficient cross-border transfers of personal data



# Summary (2/3): Comparison of Requirements between Major Certifications

There are similarities between CBPR and other certifications, except for measures to guarantee data subject's rights

✕ / ✕ : See p.60, p.86

✓ : Connection with other tools

✓ : Recommend connection with other tools

● : Applicable

			Cross-Border Transfer		Personal Data Protection Tools										
			9 APEC CBPR	10 APEC PRP	1 GDPR -CARPA	2 dp.mark	3 DPTM	4 ISMS-P	5 Privacy Mark	6 JAPHIC Mark <sup>1</sup>	7 Euro PriSe	8 TRUSTe	9 CNIL	11 China Sec. Specification	
					Based on GDPR Article46	Recommend to be obtained with CBPR	Connection with ISMS	Connection with ISMS	Based on JISQ					Defined only as relevant to the responsible person	Mandatory for data transfer
Basics	Privacy Principles	Processing Limitation	●	●	●	●	●	●	●	●	●	●	●	See following pages	●
		Notification	●		●	●	●	●	●	●	●	●	●		●
		Accuracy	●	●	●	●	●	●	●	●	●	●	●		●
		Security Safeguards	●	●	●	●	●	●	●	●	●	●	●		●
		ParticipationN/Access	●		●	●	●	●	●	●	●	●	●		●
		Harm Prevention	●												
		Accountability	●		●	3	●		3	●	3	●	3		●
	Restrictions for Sensitive Data		●		●	●	●	●	●	●	●	●	●		●
	Risk Assessment		●	●	●	●	●	●	●	●	●	●	●		●
	Record of Processing Activities		●		●	●	●	●	●	●	●	●	4		●
Tech and Org Safeguards		●	●	●	●	●	●	●	●	●	●	●	●		
Transfer/Outsource	Assessment	●		●	●		●	●	●	●	5	●	See following pages	●	
	Documentation	●		●	●	●	●	●	●	●	5	●		●	
	Supervision	●		●	●		●	●	●	●	5	●		●	
	Safeguards of Transfer	2		●	●	●	●	●	●	●	●	●		●	
	Right of Access		●		●	●	●	●	●	●	●	●		●	●
Transfer/Outsourcing	Automated Individual Decision-Making			●	●						●		●		
	Right to Object	●		●	●	●	6	●	●	●	●	●	●	●	
	Right of Data Portability			●	●	●		●	●	●	●	●	●	●	
	Children's Rights			●	●						●	●		●	

1. Use Kojouhou Tsusokukun [PIPL General Rules] 2. No applicable items, but cross-border transfers are the purpose and subject of certification and regulation in the first place.




3. Require commitment for the performance from the management level. 4. Require records only with respect to third-party provisioning activities. 5. Separate definitions for processors, joint controllers, etc. 6. The measures required to guarantee the rights of data subjects are access to personal data, correction and deletion, suspension of processing, objection, and response to requests for withdrawal of consent, with no mention of disclosure or reproduction of personal data.















































































































Source: Website of various authorities, etc.



# Summary (3/3): Comparison of Technical and Organizational Measures

GDPR-based certification is leading the way, but recently detailed requirements have also been set for other certifications

 /  : See p.60, p.86  
 : Applicable

	Cross-Border Transfer		Personal Data Protection Tools									
	9 APEC CBPR	10 APEC PRP	1 GDPR -CARPA	2 dp.mark	3 DPTM	4 ISMS-P	5 Privacy Mark	6 JAPHIC Mark <sup>1</sup>	7 Euro PriSe	8 TRUSTe	9 CNIL	11 China Sec. Specification
Pseudonymization and encryption	2				5		Only implementation of appropriate protective measures required <sup>8</sup>				Defined only as relevant to the responsible person	
Ensuring confidentiality, integrity, availability	3											
Ensuring data availability and restoration of access in event of incident												
Regular testing to ensure security of processing												
User identification and authorization												
Protection of data during transfer	 <sup>2</sup>											
Protection of data during storage												
Ensuring physical security of locations where personal data is processed		4			 <sup>6</sup>							
Ensuring event logging												
Ensuring system configuration					 <sup>7</sup>							
Internal IT and IT security governance and management												
Assurance/certification of processes/products					 <sup>7</sup>							
Data minimization												
Data quality												
Limited data retention												
Accountability												
Data portability												

Note: Compare based on EU SCC Annex II, Source: Website of various authorities, etc.

1. Use [Kojinhou Tsusokuken \[PIPL General Rules\]](#) for comparison 2. Encryption is only a limited requirement (specified as a measure for transferring or communicating personal information) ([CBPR Ninsho Kijun \[CBPR Criteria\] Annex](#)) 3. Only require "reasonable measures appropriate to the sensitivity of the personal information." ([CBPR Ninsho Kijun \[CBPR Criteria\] #6.3](#)) 4. Just required "description of physical, technical and administrative safeguards", but no specifics ([PRP Intake Questioners #2](#)) 5. There is no requirement for anonymization itself, although there is a requirement to document the policy regarding anonymization at the time of storage. ([DPTM Checklist Principle3 #5](#)) 6. Just required "administrative, technical and physical safeguards", but no specifics ([DPTM Checklist Principle3 #1](#)) 7. No specific measures are described, but data protection design during system development is required. ([DPTM Checklist Principle1 #7](#)) 8. [Privacy Mark ni okeru kojinhouhougo maneimentsisutemu kouchiku unnyoshishin \[Privacy Mark Guideline\] J.9.2](#)



# Ref.) Comparison of Requirements: Privacy Principles

In this research, we used following items as a privacy principle that organized by 3 major international privacy principles

Privacy Principles by International Organization				
Titles in this paper	OECD (8 items)	APEC (9 items)	ASEAN (7 items <sup>1</sup> )	Examples of Each Tool
Processing Limitation 	① Collection Limitation ③ Purpose Specification ④ Use Limitation	④ Use of personal Information ③ Collection Limitation	① Consent, Notification and Purpose ⑥ Retention	> <ul style="list-style-type: none"> <li>• Identification of Purpose (Privacy Mark J.8.1)</li> <li>• Purpose (EU SCC Clause 8.1)</li> </ul>
Notification/Choice/Openness 	⑥ Openness	② Notice ⑤ Choice	① Consent, Notification and Purpose	> <ul style="list-style-type: none"> <li>• Appropriate Acquisition (Privacy Mark J.8.2)</li> <li>• Transparency (EU SCC Clause 8.2)</li> </ul>
Accuracy 	② Data Quality	⑥ Integrity of Personal Information	② Accuracy of Personal Data	> <ul style="list-style-type: none"> <li>• Accuracy (Privacy Mark J.9.1)</li> <li>• Accuracy and Data Minimization (EU SCC Clause 8.3)</li> </ul>
Security Safeguard 	⑤ Security Safeguards	⑦ Security Safeguards	③ Security Safeguards	> <ul style="list-style-type: none"> <li>• Security Safeguards (Privacy Mark J.9.2)</li> <li>• Security of Processing (EU SCC Clause 8.5)</li> </ul>
Individual Participation/Access 	⑦ Individual Participation	⑧ Access and Correction	④ Access and Correction	> <ul style="list-style-type: none"> <li>• Rights Regarding Personal Information (Privacy Mark J.10.1)</li> <li>• Data Subject Rights (EU SCC Clause 10)</li> </ul>
Preventing Harm 	—	① Preventing Harm	—	> <ul style="list-style-type: none"> <li>• N/A</li> </ul>
Accountability 	⑧ Accountability	⑨ Accountability	⑦ Accountability	> <ul style="list-style-type: none"> <li>• Documentation and Compliance (EU SCC Clause 8.9a)</li> </ul>

1. ASEAN PDP Framework Principle 5 (Transfers to Another Country or Territory) has no commonality with the OECD/APEC. Thus, we organized as an item outside of the principles  
 Source: Masao H., Fumio S., Tamotsu N. "OECD Privacy Guideline-30nenn no shinka to mirai [OECD Privacy Guideline-30 years Evolution and its Future]," 2014 ; APEC "APEC Privacy Framework (2015)" 2017; ASEAN "ASEAN Telecommunications and information technology ministers meeting (TELMIN) Framework on personal data protection" 2016; European Commission "Standard Contractual Clauses (SCC)"; JIPDEC "Privacy Mark Seido [Privacy Mark System]"



## Ref.) Technical & Organizational Measures

In some cases, the tools confirm the implementation of specific measures, so we organized and compared them as follows

Technical and Organizational Measures from EU SCC	Examples of Specific Measures noted in each tool ※Black: Technical Measures, Blue: Organizational Measures, Green: Physical Measures
Pseudonymization and encryption	Encryption, Anonymization, Pseudonymization, etc.
Ensuring confidentiality, integrity, availability	Introduction of data backup system, Synchronization of each information system, etc.
Ensuring data availability and restoration of access in event of incident	Introduction of data backup system, etc.
Regular testing to ensure security of processing	Management of technical vulnerabilities, <a href="#">Implementation of periodic audits</a> , etc.
User identification and authorization	Use of ID/PW, etc.
Protection of data during transfer	Implementation of network security, Identification and management of devices for data transfer, etc.
Protection of data during storage	Introduction of data backup system , Access control, etc.
Ensuring physical security of locations where personal data is processed	<a href="#">Setup of server/computer usage area</a> , <a href="#">Access control</a> , etc.
Ensuring event logging	Creation of log files, Implementation of logging/monitoring systems, etc.
Ensuring system configuration	Implementation of data protection by default (by design), Installation of various anti-malware software (anti-malware, firewalls, etc.), Network control, etc.
Internal IT and IT security governance and management	Network management, <a href="#">Access permission management</a> , etc.
Assurance/certification of processes/products	Source program management, Test data management, <a href="#">Establishment of development processes (test, release, etc.)</a> , etc.
Data minimization	<p>The following examples are not provided because they overlap with measures to comply with the Privacy Principles and to protect the rights of data subjects.</p> <p>* In the comparison table, when there are provisions regarding measures to comply with the applicable privacy principle and measures to protect the rights of data subjects, it is judged as applicable (●).</p>
Data quality	
Limited data retention	
Accountability	
Data portability	

Note: In the EU SCC, the term "Technical and Organizational Measures" includes three types of measures: technical, organizational, and physical. In the case of cross-border transfer tools such as SCC/MCC, specific measures other than encryption requirements (e.g., network control, etc.) are rarely indicated, and the requirements are at the level of "physical measures" and "technical and administrative measures. On the other hand, general data protection tools often list more specific measures, and in such cases, the applicability to the comparison items was determined according to the organization on this page.





## 2.2

# Details of the Results: Regulations/International Rules



# Regulations & International Rules

We examined a wide range of relevant regulations

		Title	Countries/Regions	Year Issued
Regulation		1 Cross-border transfer/Localization regulations in major countries/regions	22 countries/Regions	—
International Rule		1 OECD Guidelines governing the protection of privacy and transborder flows of personal data	OECD Members	1980 (revised in 2013)
		2 Convention for the protection of individuals with regards to automatic processing of personal data (Council of Europe convention 108)	55 countries (Council of Europe 46 countries, and other 9 countries)	1985 (revised in 1999)
		3 APEC Privacy Framework	APEC Members	2004 (revised in 2016)
		4 ASEAN Framework on Personal Data Protection	ASEAN Members	2016
Trade Agreement		1 General Agreement on Trade in Services (GATS)	WTO Members	1995
		2 Regional Trade Agreement (FTA)		
		<ul style="list-style-type: none"> <li>i) Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)</li> <li>ii) Regional Comprehensive Economic Partnership Agreement (RCEP)</li> </ul>	<ul style="list-style-type: none"> <li>Japan, Singapore, Vietnam, Australia, New Zealand, Canada, Mexico</li> <li>ASEAN Members (10 countries), Japan, South Korea, China, Australia, New Zealand</li> </ul>	<ul style="list-style-type: none"> <li>2021</li> <li>2022</li> </ul>



# Overview of Regulations/International Rules (1/2)

Countries develop domestic regulations based on international rules; some countries develop GDPR-like regulations while others develop data localization



Most regulations allow for cross-border data transfer if certain requirements are met; however, its requirements vary

- 11 countries/regions require that cross-border data transfer be accompanied by the consent of the individual and that the destination country have a data protection system that is "equivalent" or "adequate" to that of the home country.
- Of the 11 countries/regions, 7 countries/regions have a system to officially certify the level of protection at the transfer destination (e.g., adequacy decision<sup>1</sup>).
  - The number becomes 8, If including the countries/regions with no "equivalent level" or "sufficient level" provision but with a similar provision ("data exporter has the same obligations as the data importer")
- There are 4 countries/regions recognize the conclusion of legally binding documents between the parties, certification and seals, and codes of conduct<sup>2</sup> as requirements for cross-border data transfers, in addition to consent and an "equivalent" or "sufficient level" of protection. All of them have developed regulations in line with the GDPR.
- Exceptionally, there are some countries/regions that do not have specific requirements for the cross-border transfer.



Not many countries/regions have data localization regulations, but some countries/regions, including China and Russia, have established cross-border transfer regulations as well as in-country storage of data, etc.

- There are some countries/regions that have no regulations on cross-border transfer of personal data but have only localization regulations



Some requirements apply to multiple countries, especially as international rules are the basis for all requirements and interact with national/regional regulations.

- Some requirements apply to multiple countries, and in particular, international rules interact with national/regional regulations as the basis for all requirements

1. A system whereby the responsible authority in each country/region certifies that the subject of personal data handling has an adequate level of personal data protection in light of its criteria. Upon certification of sufficiency, the transfer of personal data to the subject is permitted. 2. Rules and policies for the protection of personal data established by businesses and organizations



# Overview of Regulations/International Rules (2/2)

The main requirements for cross-border data transfer/data localization in each domestic law are as follows:

		Cross-Border Data Transfer Requirements							Data Localization Requirements
		Consent	Protection at destination	Contract	Cert., etc.			CoC	Others
			Adequate level	Adequacy Decision	Legally binding Documents	SCC	BCR	Others	
Countries/Regions with regulations like GDPR	EU	●		●	●	●	●	●	● Arrangements, Authority Approval
	UK			●	●	●	●	●	● Other provisions/arrangements
	Singapore	●	●		●	●	●		● Authority Approval
	Brazil	●		●	●	●	●	●	● Authority Approval, etc.
Countries/Regions requiring "equivalent" or "adequate" level of protection	Japan	●	●	●					● <sup>1</sup>
	New Zealand	●	●	●					
	Australia	●	●						● Court approval, etc.
	Thailand	●	●				●		
	South Africa	●	●		●		●		● Required by contracts, etc.
	Mexico	●	●						
	Turkey	●		●					● Written and Authority Approval
	China	●			●	●			● Authority Approval, etc.
Countries/Regions with data localization	Russia	●	● <sup>2</sup>	● <sup>2</sup>	●				● Authority Approval, etc.
	Indonesia	●	●		●				● Linkage to ministers, agreement between nations
	South Korea	●							● Installation of institutional technical measures <sup>3</sup>
	Vietnam								● Stipulated by individual/field law
	India								● Stipulated by individual/field law
	Saudi Arabia								● Life safety and other specific situations
									● No applicable regulation, but substantially restricted
Countries/Regions without related regulations	Canada, Taiwan, United States, Philippines	No applicable regulation							

1. Guidelines allow the use of CBPR (*Kojinjouhou no hogo ni kannsuru houritsu ni tsuite no gaidorainn* [Personal Information Guidelines (Provision to a third party located in a foreign country, ed.), 2019]) 2. Allow transfer to the Convention 108 member countries 3. For important data





## Details of the Results: Regulations

We provide the following details on the next page

		Title	Countries/Regions	Year Issued
Regulation		1 Cross-border transfer/localization regulations in major countries/regions	22 countries/Regions	—
International Rule		1 OECD Guidelines governing the protection of privacy and transborder flows of personal data (OECD Privacy Guidelines)	OECD Members	1980 (revised in 2013)
		2 Convention for the protection of individuals with regards to automatic processing of personal data (Council of Europe Convention 108)	55 countries (Council of Europe 46 countries, and other 9 countries)	1985 (revised in 1999)
		3 APEC Privacy Framework	APEC Members	2004 (revised in 2016)
		4 ASEAN Framework on Personal Data Protection (ASEAN PDP Framework)	ASEAN Members	2016
Trade Agreement		1 General Agreement on Trade in Services (GATS)	WTO Members	1995
		2 Regional Trade Agreement (FTA)		
		i) Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)	Japan, Singapore, Vietnam, Australia, New Zealand, Canada, Mexico	2021
		ii) Regional Comprehensive Economic Partnership Agreement (RCEP)	ASEAN Members (10 countries), Japan, South Korea, China, Australia, New Zealand	2022





# Countries/Regions with regulations like GDPR (1/4)



EU

## Cross-Border Data Transfer Regulations

### Applicable Regulation

- GDPR (General Data Protection Regulation)
  - Issued 2016, enforced 2018

### Target data

- any information relating to an identified or identifiable natural person ('data subject') (Article 4(1))
  - an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4(1))

### Regulated persons

- Controller (Article 4(7))
  - The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
- Processor (Article 4(8))
  - A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

### Cross-Border Data Transfer Requirements

Cross-border data transfer prohibited in general, but possible if any of the following requirements are met (Article 44)

- ① Transfers on the basis of an adequacy decision (Article 45)
- ② Transfers subject to appropriate safeguards (Article 46)
  - In the absence of an adequacy decision, a controller or processor may transfer only if they have provided any of b-h in addition to a
    - a. Enforceable data subject rights and effective legal remedies for data subjects
    - b. A legally binding and enforceable instrument between public authorities or bodies
    - c. Binding corporate rules (BCR)
    - d. Standard Contractual Clauses (SCC)
    - e. SCC adopted by a supervisory authority and approved by the Commission
    - f. An approved Codes of Conduct
    - g. An approved certification mechanism with commitments of the controller or processor in the third country
    - h. Contractual clauses or arrangements with authorization from the supervisory authority
- ③ Derogations for specific situations (Article 49)

## Data Localization Regulations

### Applicable Regulation

No applicable regulation





# Countries/Regions with regulations like GDPR (2/4)

## United Kingdom

### Cross-Border Data Transfer Regulations

There are two personal data protection regulations in the UK: the UK GDPR and the DPA2018. the DPA2018 sets the framework for data protection law in the UK and is parallel to and complementary to the UK GDPR. Since the UK GDPR and DPA2018 provide for almost the same content with respect to cross-border transfers, this section will focus on the UK GDPR.

#### Applicable Regulation

General Data Protection Regulation: UK GDPR  
 - Enforced in 2021

#### Target data

Any information relating to an identified or identifiable natural person ('data subject') (Article 4(1))

- an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4(1))

#### Regulated persons

- Controller (Article 4(7))  
 The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
- Processor (Article 4(8))  
 A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Source: [UK GDPR](#); [Data Protection Act 2018](#)

### Cross-Border Data Transfer Requirements

Cross-border data transfer prohibited in general, but possible if any of the following requirements are met (Article 44)

- ① Transfers on the basis of an adequacy decision (Article 45)
- ② Transfers subject to appropriate safeguards (Article 46)  
 In the absence of a decision on sufficiency, cross-border transfers can be made by providing b-h in addition to a
  - a. effective legal remedies for data subjects
  - b. a legally binding and enforceable instrument between public authorities or bodies
  - c. Binding corporate rules
  - d. SPDC (Standard Data Protection Clauses) by 17C or 119A of DPA 2018
  - e. Approved Codes of Conduct
  - f. Approved certification mechanism
  - g. Other individual contractual provisions or arrangements
- ③ Derogations for specific situations (Article 49)

### Data Localization Regulations

#### Applicable Regulation

No applicable regulation





# Countries/Regions with regulations like GDPR (3/4)



Singapore

## Cross-Border Data Transfer Regulations

The implementing regulation provides the details. Therefore, we introduce the implementing regulation (PDPR) in addition to the comprehensive act (PDPA)

### Applicable Regulation ①

Personal Data Protection Act 2012 (PDPA)

- Enforced in 2012, revised in 2020

### Target data

The data, whether true or not, about an individual who can be identified from that data or from that data and other information to which the organization has or is likely to have access (Article 2)

### Regulated persons

Businesses

- includes the activity of any organization, whether or not carried on for purposes of gain, or conducted on a regular, repetitive or continuous basis, but does not include an individual acting in his or her personal or domestic capacity (Article 2)

### Cross-Border Data Transfer Requirements

Cross-border data transfer prohibited in general, but possible if any of the following requirements are met (Article 26)

- ① Provide a standard of protection to personal data so transferred that is comparable to the protection under this Act.
- ② Approval from Personal Data Protection Commission (PDPC)

### Applicable Regulation ②

Personal Data Protection Regulations 2021 (PDPR)

- Enforced in 2021

### Target data/Regulated Persons

Same as PDPA

### Cross-Border Data Transfer Requirements

- Transfers are possible with implementation of the following "appropriate measures to ensure a legally binding obligation to provide a level of protection equivalent to that of the PDPA" (Article 10,11)
  - ① Any law
  - ② Any contract
  - ③ Any binding corporate rules (BCR)
  - ④ Any other legally binding instrument
  - ⑤ Approved certifications: CBPR and PRP
- The obligation to restrict data transfers may also be deemed to be satisfied if (Article 10)
  - ⑥ Consent of data subject is given
  - ⑦ It is necessary for the benefit of the individual/state and reasonable steps are taken
  - ⑧ The personal data is data in transit
  - ⑨ The personal data is publicly available in Singapore

## Data Localization Regulations

### Applicable Regulation

No applicable regulation





# Countries/Regions with regulations like GDPR (4/4)



## Brazil

### Cross-Border Data Transfer Regulations

#### Applicable Regulation

- Personal Data Protection Law (Lei Geral de Proteção de Dados Pessoais: LGPD)
  - Enforced in 2018

#### Target Data

Information about an identified or potentially identified natural person (Article 5, paragraph 1)

#### Regulated Persons

- Controller: A natural or legal person responsible for making decisions regarding the processing of personal data (Article 5 (6))
- Processor: The natural or legal person processing personal data on behalf of the controller (Article 5 (7))

### Cross-Border Data Transfer Requirements

Cross-border data transfer is possible if any of the following requirements are met (Article 33-36)

- ① The country/international organization where data is transferred has a personal data protection regime comparable to that of LGPD<sup>1</sup>
- ② The controller guarantees or certifies in the following compliance with the principles stipulated, the rights of data subjects, and the data protection regime
  - a. Specific contractual clause for a particular transfer
  - b. Standard contractual clauses
  - c. Binding corporate rules
  - d. Seals, certificates and codes of conduct

- ③ The transfer is necessary for the purpose of international judicial assistance
- ④ The transfer is necessary for the life or physical safety of the owner or a third party
- ⑤ The transfer has been approved by the data protection authority (Autoridade Nacional de Proteção de Dados: ANPD)
- ⑥ The transfer is necessary in accordance with a commitment agreed to in an international agreement etc.
- ⑦ The transfer is necessary for the implementation of public policy or services
- ⑧ Consent (However, only with prior information sharing on the international nature of transfer and consent independent of other purposes)
- ⑨ The transfer is necessary for compliance with the obligations of the controller under law
- ⑩ The transfer is necessary for the conclusion, performance, and prep of a contract to which the data subject is a party, in accordance with the data subject's request
- ⑪ The transfer is necessary for the normal exercise of rights in judicial/administrative proceedings

### Data Localization Regulations

#### Applicable Regulation

No applicable regulation

1. ANPD is responsible for evaluating the level of data protection in the target country (e.g., making an adequacy decision)(Article 34)

Source: [Lei Geral de Proteção de Dados Pessoais \[Personal Data Protection Law\]](#)





# Countries/Regions requiring "equivalent"/"adequate" level of protection (1/7)

## Japan

### Cross-Border Data Transfer Regulations

---

#### Applicable Regulation

- Act on the Protection of Personal Information (APPI)
- Promulgated in 2003, enforced in 2005
  - Amended in 2015, enforced in 2017
  - Amended in 2020, enforced in 2022

#### Target Data

Information that can be used to identify a specific individual, including information that can be easily cross-checked with other information and thereby used to identify a specific individual (Article 2 (1))

#### Regulated Persons

Personal data processing business (Article 16, (2))  
Those who use databases etc. containing personal data for business purpose. However, national orgs, local governments, and independent administrative agencies are excluded

#### Cross-Border Data Transfer Requirements

Cross-border data transfer is possible only if any of the following requirements are met (Article 28 (1))

- ① Consent of the person
- ② The country where data is transferred is a foreign country that has a system for the protection of personal data, recognized as being at the same level as that of Japan as stipulated in the rules of the personal data protection commission
- ③ The business where data is transferred is a business entity that has established a system that complies with the standard for privacy protection set forth in the personal data protection commission's rules

### Data Localization Regulations

---

#### Applicable Regulation

No applicable regulation





# Countries/Regions requiring "equivalent"/"adequate" level of protection (2/7)



## New Zealand

### Cross-Border Data Transfer Regulations

#### Applicable Regulation

- Privacy Act 2020
  - Enforced in 2020

Persons subject to the Privacy Act are required to comply with the Information Privacy Principles (IPP). The contents of the IPP are incorporated in Article 22 of the Privacy Act.

#### Target Data

Information about an identifiable individual including information relating to a death (Article 7)

#### Regulated Persons

Domestic and foreign businesses, regardless of whether they are registered in the country (Article 4)

### Cross-Border Data Transfer Requirements

Cross-border data transfer is possible only if any of the following requirements are met (Article 22 IPP12)

- ① Obtained the Consent of the data subject after notifying the data subject that it may not be provided equivalent protection measures
- ② Obligated the transferee equivalent level of data protection same as the Privacy Act
- ③ The data is transferred to a third party that stores or processes the data
- ④ Disclosed to the transferee in a country recognized by the government as having equivalent safeguards to those in New Zealand
- ⑤ Other exceptions

### Data Localization Regulations

#### Applicable Regulation

No applicable regulation





# Countries/Regions requiring "equivalent"/"adequate" level of protection (3/7)



## Australia

### Cross-Border Data Transfer Regulations

Personal data protection regulation in Australia consists of both comprehensive law (APA) and individual laws. There are regulations (e.g., Spam Act 2003) that govern the handling of personal data by specific businesses, and several state laws also contain personal data provisions. This section introduces the APA, Australia's primary personal data protection regulation. As in New Zealand, APA subjects are required to comply with the Australian Privacy Principles (APP), which are included in the APA.

#### Applicable Regulation

Australia Privacy Act 1988 (APA)

- Since the first edition in 1988, it has undergone several minor revisions, with the latest edition coming into effect in 2022

#### Target Data

Information or an opinion about an identified individual, or an individual who is reasonably identifiable (Article 6):

- Whether the information or opinion is true or not; and
- Whether the information or opinion is recorded in a material form or not

#### Regulated Persons

All businesses with annual sales of A\$3 million or more (Article 6D)

- Organization includes: an individual, a body corporate, a partnership, any other unincorporated association, a trust, and state or territory authority (Article 6C)

### Cross-Border Data Transfer Requirements

- Cross-border data transfer is possible only if reasonable measures are in place to ensure that the transfer does not violate the APP (Schedule1 8.1)
- However, exceptions may be made in the following cases (Schedule1 8.2)
  - ① The recipient is subject to a personal data protection scheme/tool similar to APP
  - ② With an explicit statement that APP 8.1 is no longer applicable and the consent of the individual
  - ③ Required by or under an Australian law or a court/tribunal order
  - ④ Necessary to mitigate or prevent a serious threat to life, health, or safety
  - ⑤ Necessary to take action against illegal activities or suspected illegal activities
  - ⑥ Necessary to locate a missing person

### Data Localization Regulations

#### Applicable Regulation

No applicable regulation





# Countries/Regions requiring "equivalent"/"adequate" level of protection (4/7)

## Thailand

### Cross-Border Data Transfer Regulations

#### Applicable Regulation

- Personal Data Protection Act, B.E. 2562 (PDPA)
  - Partially enforced in 2019, completely enforced in 2022

The Personal Data Protection Committee (PDPC) of Thailand is expected to establish the details of Thailand's PDPA in a subordinate regulation. However, as of September 2022, no applicable sub regulations have been enacted. Therefore, only the details of the cross-border transfer regulations stipulated in the PDPA are presented here.

#### Target Data

Any information relating to a Person, which enables the identification of such Person, whether directly or indirectly, but not including the information of the deceased Persons in particular (Section 6)

#### Regulated Persons

- Data Controller (Section 6)
  - A person or a juristic person having the power and duties to make decisions regarding the collection, use, or disclosure of the personal data Data
- Processor (Section 6)
  - A Person or a juristic person who operates in relation to the collection, use, or disclosure of the Personal Data pursuant to the orders given by or on behalf of a Data Controller, whereby such Person or juristic person is not the Data Controller

\* The regulation also applies to foreign controllers and processors when they provide services to data subjects located in Thailand. (Section 5)

#### Cross-Border Data Transfer Requirements

Cross-border data transfer is prohibited in general, but possible if all the following requirements are met (Section 28, 29)

- The destination country or region meets "adequate data protection standards"
- Transfers are made in accordance with the regulations established by the PDPC. However, cross-border transfers are possible if one of the following requirements is met
  - If any of the following exceptions apply:
    - For compliance with the law
    - When the data subject's consent is obtained after being notified that the transferee does not have adequate personal data protection measures
    - 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
    - For compliance with a contract between the Data Controller, and other Persons or juristic person for the interests of the data subject
    - Necessary to prevent or mitigate damage to the life, body, or health of the data subject or others, where the consent of the data subject cannot be obtained at the time
    - Necessary for carrying out the activities in relation to substantial public interest.
  - Transfer is between group entities and the parties have a data protection policy approved by the Personal Data Protection Commission

### Data Localization Regulations

#### Applicable Regulation

No applicable regulation

Source: Personal Data Protection Act, B.E. 2562 (2019); JETRO "Kojinjouhou hogohou ga 6gatsu kara kannzenn shikou (Tai) [The Personal Information Protection Law will be fully enforced from June (Thailand)]." 2022





# Countries/Regions requiring "equivalent"/"adequate" level of protection (5/7)

## South Africa

### Cross-Border Data Transfer Regulations

#### Applicable Regulation

Protection of Personal Information Act (PoPIA)

- Partially enforced in 2013, completely in enforced 2021

#### Target Data

Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person (Section 1)

#### Regulated Persons

- Responsible Party (Section 1)  
A public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information
- Operator (Section 1)  
A person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party

### Cross-Border Data Transfer Requirements

Cross-border data transfer is possible only if any of the following requirements are met (Section 72)

- ① BCR or binding agreement which provide an adequate level of protection
- ② The data subject consents to the transfer
- ③ Necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request

- ④ Necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party or for benefit of the data subject
- ⑤ Necessary for the benefit of the data subject, and not reasonably practicable to obtain the consent of the data subject to that transfer

### Data Localization Regulations

#### Applicable Regulation

No applicable regulation





# Countries/Regions requiring "equivalent"/"adequate" level of protection (6/7)



## Mexico

### Cross-Border Data Transfer Regulations

#### Applicable Regulation

- Private Retained Personal Data Protection Law  
(Ley Federal de Protección de Datos Personales en Posesión de los Particulares)
  - Enforced in 2010

#### Target Data

Any information about an identified or identifiable natural person (Article 3 (5))

#### Regulated Persons

- Controller (Article 3 (14))  
A natural or legal person of a private nature who decides on the processing of personal data
- Processor (Article 3 (9))  
A nature or legal person or entity acting alone or jointly with others on behalf of the controller
- Third party (Article 3 (16))  
Any nature or legal person other than the controller or the controller, whether domestic or foreign

#### Cross-Border Data Transfer Requirements

- Cross-border data transfer is possible only if all the following requirements are met (Article 36)
  - ① Consent is obtained
  - ② Domestic and foreign third parties have the same obligations as the controller

- However, if any of the followings apply, ① obtaining consent is not required (Article 37)
  - a. Stipulated in laws or treaties
  - b. Data is transferred within the same group
  - c. Necessary to maintain a legal relationship or contract between the controller and the data subject or third party where data is transferred
  - d. Other: Necessary for medical services, public interest, judicial proceedings

### Data Localization Regulations

#### Applicable Regulation

No applicable regulation





# Countries/Regions requiring "equivalent"/"adequate" level of protection (7/7)



## Turkey

### Cross-Border Data Transfer Regulations

#### Applicable Regulation

- Law on Protection of Personal Data (LPPD)
  - Enforced in 2016

#### Target Data

Any information about an identified or identifiable natural person (Article 3)

#### Regulated Persons

- Data Controller (Article 3)
  - Natural or legal persons responsible for determining the purposes and measures of processing personal data and for establishing and managing the system
- Data Processor (Article 3)
  - Natural or legal persons that process personal data based on the controller's authorization

### Cross-Border Data Transfer Requirements

- Cross-border data transfer is possible only with the explicit consent of the person in question (Article 9 (1))
- However, cross-border transfers without consent are possible if exceptions to processing (Article 5 (2) and Article 6 (3)) apply and one of the following requirements is also met (Article 9 (2))
  - ① The country where data is transferred provides adequate personal data protection measures<sup>1</sup>
  - ② The domestic or foreign controller confirms in writing that it provides adequate protection and DPB approve it

1. Target countries are reviewed/determined by Data Protection Board (DPB)

Source: [Personal Data Protection Authority "Personal Data Protection Law"](#)

### Data Localization Regulations

#### Applicable Regulation

No applicable regulation





# Countries/Regions with data localization (1/11)



## China

### Cross-Border Data Transfer Regulations

#### Applicable Regulation ①

- Personal Information Protection Law (PIPL)
  - Enforced in 2011

#### Target Data

Non-anonymized information of any kind relating to an identified or identifiable natural person that is recorded electronically or otherwise (Article 4)

#### Regulated Persons

- Processor (Article 73 (1))
  - Organizations or individuals who independently determine the purpose and measures of processing personal data

#### Cross-Border Data Transfer Requirements

In addition to obtain consent (Article 39), cross-border data transfer is possible only if any of the following requirements are met (Article 38)

- ① Pass the security evaluation by National internet information department
- ② Certified by National internet information department
- ③ Concluded a standard contract with the business who receives transferred data
- ④ Comply with other laws (international treaties etc.)

#### Applicable Regulation ②

- Cyber Security Law (CSL)
  - Enforced in 2017

#### Target Data

- Personal data (Article 76 (5))
  - Various types of information that can be recorded by electronic data or other means and that can be used alone or in combination with other information to identify the identity of a natural person
- Important data

#### Regulated Persons

Important data infra operators (Article 37)

#### Cross-Border Data Transfer Requirements

Safety assessment must be conducted if business needs require provision outside of the country (Article 37)





# Countries/Regions with data localization (2/11)



## China

### (Continued) Cross-Border Data Transfer Regulations

#### Applicable Regulation ③

- Data Security Law (DSL)
- Enforced in 2021

#### Target Data

- Data belonging to controlled items related to the protection of national security and interests and the fulfillment of international obligations (Hereafter, data belonging to controlled items)
- Important data

#### Regulated Persons

Regulations vary depending on the type of data

- Data belonging to controlled items: Processor
- Important data: Important data infra operators, other processors

#### Cross-Border Data Transfer Requirements

Regulations vary depending on the type of data

- Data belonging to controlled items : Implement export control (Article 25)
- Important data: Regulations differ depending on the type of subject
  - Important data infra operators: Comply with the cyber security law (Article 31)
  - Other processors: Follow the measures established by the national network department with the relevant departments (Article 31)

### Data Localization Regulations

#### Applicable Regulation ①

- Personal Information Protection Law (PIPL)
- Enforced in 2011

#### Target Data

Non-anonymized information of any kind relating to an identified or identifiable natural person that is recorded electronically or otherwise (Article 4)

#### Regulated Persons

- National institutions
- Important data infra operators
- Processors that process more personal data than no. of defined by National Internet information department
- Processors who provide personal data stored in the country to foreign judicial or law enforcement agencies

#### Cross-Border Data Transfer Requirements

- In principle, personal data is stored domestically. Cross-border data transfer is possible only in the following:
  - National institutions/important data infra operators/processors who process more than a certain amount of level:
 

Cross-border transfers are possible only after passing a security evaluation
  - Processors who provide personal data to foreign institutions:
 

Cross-border transfers are possible only with the approval of competent authorities





# Countries/Regions with data localization (3/11)



## China

### (Continued) Data Localization Regulations

#### Applicable Regulation ②

- Cyber Security Law (CSL)
  - Enforced in 2017

#### Target Data

- Personal data (Article 76(5))
  - Various types of information that can be recorded as electronic data or other means and that can be used alone or in combination with other information to identify the identity of a natural person
- Important data

#### Regulated Persons

Important data infrastructure operators (Article 37)

#### Cross-Border Data Transfer Requirements

Important data infrastructure operators must store important data and personal data collected in-country (Article 37)

#### Applicable Regulation ③

- Data Security Law (DSL)
  - Enforced in 2021

#### Target Data

Important data

\* However, no specific mention of regulated data for domestic organizations or individuals in the following section

#### Regulated Persons

- Important data infrastructure operators (Article 31)
- Other processors (Article 31)
- Domestic organizations or individuals (Article 36)

#### Cross-Border Data Transfer Requirements

Regulations vary depending on those being regulated

- Important data infrastructure operators
  - Comply with cyber security law (Article 31)
- Other processors
  - Follow the means established by national network department together with relevant departments (Article 31)
- Domestic organizations or individuals
  - Need approval from the competent authorities is required for provision to foreign government agencies (Article 36)





# Countries/Regions with data localization (4/11)



## Russia

### Cross-Border Data Transfer Regulations

#### Applicable Regulation

- Federal Law on Personal Data (no.152-FZ)
- Enforced in 2006

#### Target Data

Any information referring directly or indirectly to a particular or identified private entity (data subject) (Article 3(1))

#### Regulated Persons

Controller (Article 3(2))

The state body, municipal body, legal entity or private entity that, independently or in conjunction with other entities, organizes/processes personal data and determines the purposes of personal data processing, the composition of the personal data to be processed, and the actions (operations) performed during personal processing

#### Cross-Border Data Transfer Requirements

Cross-border data transfer is possible only if any of the following requirements are met (Article 12)

- ① Transfer to the parties of the Council of Europe Convention
- ② Countries approved by the authorities as having an adequate level of protection
- ③ Consent of data subject
- ④ Stipulated by international agreements of the Russia
- ⑤ Necessary to ensure national defense and state security

- ⑥ For the purpose of the execution of an agreement to which the data subject is a party
- ⑦ For the purpose of protecting the life, health or other vital interests of the
- ⑧ Data subject or other entities if it is not possible to obtain the written consent of the data subject

### Data Localization Regulations

#### Applicable Regulation

- Federal Law on Personal Data (no.152-FZ): ロシア連邦法第152-FZ号)
- Enforced in 2006

#### Target Data/Regulated Persons

Same as the left

#### Cross-Border Data Transfer Requirements

When collecting personal data, including through the network, the controller is obliged to use databases located within the country except for the following (Article 18(5))

- ① Necessary to fulfill a purpose stipulated by an international agreement/law
- ② Necessary for the controller to exercise or perform a function, authority or duty imposed on him by law
- ③ Necessary for the court proceedings
- ④ Necessary for the purposes of state administration and municipal services
- ⑤ Necessary for the purposes of creative activity





# Countries/Regions with data localization (5/11)

## Indonesia

### Cross-Border Data Transfer Regulations

#### Applicable Regulation ①

- Minister of Communications and Informatics Regulation No. 20 of 2016 on the Protection of Personal Data in an Electronic System (2016 Regulation)
- Enforced in 2016

#### Target Data

Certain personal data stored and controlled, information for which confidentiality must be protected (Article 1 (1))

#### Regulated Persons

- Electronic system provider
- The term “electronic system provider” refers to individuals, entities, and organizations that provide, manage, and operate electronic systems for needs of service users etc., either alone or jointly with others (Article 1 (6))

#### Cross-Border Data Transfer Requirements

Cross-border data transfer is possible in cooperation with the minister of information and communication (Article 22 (1)). Contents of collab are as follows (Article 22 (2))

- ① Report on the country where data is transferred, the recipient of the transfer, the date of transfer, the reason for the transfer, and the implementation plan
- ② Request for assistance as necessary
- ③ Report results of the transfer

#### Applicable Regulation ②

- Personal Data Protection Act (PDPA)
- Enforced in 2022

#### Target Data

Information about individuals or identifiable directly or indirectly through electronic or non-electronic systems (Article 1 (1))

#### Regulated Persons

Controller (Article 49)

#### Cross-Border Data Transfer Requirements

Cross-border data transfer is possible only if any of the following requirements are met (Article 49)

- ① The country where data is transferred has a personal data protection system equivalent or superior to that of Indonesia
- ② National agreement between Indonesia and the country where data is transferred
- ③ Concluded contract for data processing between the origin / the country where data is transferred
- ④ Consent of the data subject

Indonesia's long-considered PDPA was ratified on Sep 20, 2022. Scheduled to be applied after a grace period of two years.<sup>1</sup> Details, incl. cross-border transfers (Article 49), will be stipulated in the subordinate regulations

1. Hunton Andrews Kurth "Indonesia Enacts its First Data Protection Act" 2022





# Countries/Regions with data localization (6/11)

## Indonesia

### Data Localization Regulations

#### Applicable Regulation

- Government Regulation No.71 of 2019 on the Administration of Electronic Systems and Transactions (2019 government ordinance)
- Enforced in 2019

#### Target Data

No specific mention of data subject to localization regulation

#### Regulated Persons

Public sector electronic systems providers (Article 20 (2))

#### Details of cross-border transfer requirements

- Public sector electronic system providers are obliged to manage, process or store electronic systems and electronic data in Indonesia (Article 20 (2))
- However, if the committee finds that the relevant storage technology is not available in Indonesia, storage outside the country is permitted (Article 20 (3-4))

## South Korea

### Cross-Border Data Transfer Regulations

#### Applicable Regulation ①

- Personal Information Protection Act (PIPA)
- Enforced in 2020

#### Target Data

Information that identifies a particular individual, and that can be easily combined with other information to identify an individual, including pseudonym information (Article 2 (1))

#### Regulated Persons

Personal Information Controller (Article 2 (5))

A public institution, legal person, organization, individual, etc. that processes personal information directly or indirectly to operate the personal information files as part of its activities

#### Details of cross-border transfer requirements

Cross-border data transfer is possible only if notify data subject all the following items and obtaining the consent of the data subject (Article 17 (2))

- ① The purpose of use
- ② Personal information to be provided
- ③ Storage/Using period
- ④ The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent





# Countries/Regions with data localization (7/11)



## South Korea

### (Continued) Cross-Border Data Transfer Regulations

#### Applicable Regulation ②

Act on Promotion of Information and Communications Network Utilization and Information Protection

- Since first edition in 1987, it has undergone several minor revisions, with the latest edition coming into effect in 2020

#### Target Data

Important Data (Article 51(1))

- Information related to the national security and major policies
- Information about details of cutting-edge science and technology or equipment developed within this country

#### Regulated Persons

- The provider of information and communications services
- The user of information and communications services

#### Cross-Border Data Transfer Requirements

Cross-border data transfer is possible only if all the following requirements are met (Article 51(3))

1. Installation of a systematic or technical device for preventing unlawful use of information and communications networks
2. Systematic and technical measures for preventing unlawful destruction or manipulation of information
3. Measures for preventing leakage of important information that providers of information and communications services have learned while managing the information

### Data Localization Regulations

#### Applicable Regulation

No applicable regulation

There is no comprehensive law requiring domestic storage of data, but some individual laws require it in specific cases.<sup>1</sup>

- When providing cloud services to government agencies and public institutions
- For computer rooms of financial institutions headquartered in Korea and disaster recovery centers
- When medical institutions manage and supplement their electronic medical record systems and their backup devices externally

1. JETRO "Dennshi Shotorihiki no TPP3gensoku to chugoku kankoku no houseido no hikaku [Comparison of e-commerce "TPP 3 Principles" and legal systems in China and South Korea]," 2019  
Source: Act on Promotion of Information and Communications Network Utilization and Information Protection





# Countries/Regions with data localization (8/11)

## Vietnam

### Cross-Border Data Transfer Regulations

Since there are no cross-border transfer requirements now, a draft currently under consideration is presented for reference

#### Ref.) Applicable Regulation

Draft Decree on Personal Data Protection (PDPD draft)

- Call for comments in 2021

#### Target Data

Information about an individual or information that can identify a specific individual (Article 2 (1))

#### Regulated Persons

All domestic and foreign institutions, organizations, and individuals doing business in Vietnam (Article 1 (1))

#### Cross-Border Data Transfer Requirements

- Cross-border data transfer is prohibited in general, but possible if any of the following requirements are met (Article 21 (1-2))
  - ① Obtained data subject's consent
  - ② Stored original data in the country
  - ③ Proof that the country where data is transferred has a protection system of the same or higher standard than that of the home country
  - ④ Obtained written approval from personal data protection commission

- Cross-border data transfer is possible if any of the following ①-④ and ⑤⑥ are met (Article 21 (3-5))
  - ① Obtained data subject's consent
  - ② Obtained written approval from personal data protection commission
  - ③ Processor's commitment to personal data protection
  - ④ Processor's commitment to apply personal data protection measures
  - ⑤ Establishment of a system for storing transfer history in the country where data is transferred (3 yrs.)
  - ⑥ Implementation of annual periodic evaluation by personal data protection committee in the country where data is transferred





# Countries/Regions with data localization (9/11)

## Vietnam

### Data Localization Regulations

---

#### Applicable Regulation ①

- Law on Cyber Security  
- Enforced in 2019

#### Target Data

Personal data or data relating to the relationship of service users or data created by domestic service users (Article 26 (3))

#### Regulated Persons

Domestic and foreign operators that provide services or additional services on domestic telecommunication networks, the internet and in cyberspace (Article 26 (3))

#### Cross-Border Data Transfer Requirements

- If the relevant data is processed, it must be stored in the country for a certain period (Article 26 (3))
- Foreign operators that meet the requirements are obliged to set up a domestic office or branch in Vietnam (Article 26 (3))

#### Applicable Regulation ②

- Decree No.72/2013/ND-CP  
- Enforced in 2013

#### Target Data

Information on internet services, online information, and online games

#### Regulated Persons

Online service providers (Article 24-25, Article 28)

#### Cross-Border Data Transfer Requirements

Obligated to install at least one server system in Vietnam to inspect, store, and provide information as required by the competent authorities and to resolve customer complaints regarding service provision (Article 24-25, Article 28)





# Countries/Regions with data localization (10/11)



## India

### Cross-Border Data Transfer Regulations

#### Applicable Regulation

- No applicable regulation
- Information Technology Rules 2011, which are partly based on information Technology Act 2000 and partly on the detailed enforcement regulations, provide that data transfers in general “shall be permitted only where necessary for the performance of a lawful contract between a corporation or a person on behalf of a corporation and an information provider, or where this person has consented to such data transfer” (Article 7)

India’s first comprehensive law on personal data, Personal Data Protection Bill 2019 (PDPB), was put on the agenda for discussion. It was drafted after the GDPR-based 2018 draft and was expected to have stricter and broader personal data provisions, but in Aug 2022, the draft was withdrawn, and a new bill was scheduled to be submitted<sup>1</sup>

### Data Localization Regulations

#### Applicable Regulation ①

Decree on the preservation of payment system information (DL Regulations)

#### Target Data

End-to-end transaction details and information on payment or settlement transactions collected/sent/processed as part of payment messages/instructions (Article 2 (1))

#### Regulated Persons

All payment system providers approved by the reserve bank of India (RBI)

#### Cross-Border Data Transfer Requirements

All payment system providers must ensure that all data related to the systems they operate is stored exclusively on systems in India (Article 2 (1))

#### Applicable Regulation ②

License Agreement for Unifies License

#### Target Data

All financial and user information of the user, except international roaming and billing (Article 39.23 (8))

#### Regulated Persons

Licensed telecommunications service providers

#### Cross-Border Data Transfer Requirements

Prohibit the transfer of information out of the country (Article 39.23 (8))

1. TMI Associates, “Indo saishin hourei jouhou - (2022nenn 8gatsu gou) Indo kojinjouhou hogo houann no hakushitekkai [India’s latest legal news - (Aug 2022) India personal data protection law proposal withdrawn],” 2022

Source: Reserve Bank of India “Storage of Payment System Data”; Government of India Ministry of Communications & IT Dept. of Telecommunications “License Agreement for Unifies License”





# Countries/Regions with data localization (11/11)

## Saudi Arabia

### Cross-Border Data Transfer Regulations

#### Applicable Regulation

Personal Data Protection Law (PDPL)

- Promulgated in 2022, scheduled to be effective in March 2023

#### Target Data

All information that leads to or can directly or indirectly identify an individual (Article 1)

#### Regulated Persons

Controller (Article 1)

### Cross-Border Data Transfer Requirements

- Cross-border data transfer is possible only when necessary to protect the life or vital interests of the data subject and to prevent or treat infection (Article 29)
- However, if it is for the performance of obligations under a contract to which the country is a recipient, or for the national interest or for any other purpose provided for in the regulations, cross-border transfers are possible if all the following requirements are met (Article 29)  
(Any of the requirements except ① may be waived if approved by the competent authority)
  - ① National security or vital interests of the country are not impaired by transfer/disclosure
  - ② Provision of adequate assurance that the personal data will not fall below the order of protection required by law and regulation to maintain the data's confidentiality
  - ③ Minimum required personal data to be transferred or disclosed
  - ④ Authorized by the competent authorities

### Data Localization Regulations

#### Applicable Regulation

No applicable regulation

Although there are no localization requirements, the regulation is effectively based on domestic preservation, as the requirements for the approval of cross-border transfers are quite limited.<sup>1</sup>

1. [White Label Consultancy "Saudi Arabia Data Protection Law" 2022](#)  
Source: [Saudi Arabia Government "Personal Data Protection Law \[Published in Arabic\]"](#)





# Countries/Regions without related regulations (1/3)



Canada

## Cross-Border Data Transfer Regulations

### Applicable Regulation

Personal Information Protection and Electronic Documents Act (PIPEDA)

- Issued in 2000, completely enforced in 2004
- Frequently revised and amended, latest edition is 2019

### Target Data

Information about an identifiable individual (Article 2 (1))

### Regulated Persons

Every organization in respect of personal information except the following (Article 4(1)(2))

- Any government institution to which the Privacy Act applies
- Any individual collects, uses or discloses for personal/domestic purposes
- Any organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose

### Cross-Border Data Transfer Requirements

- PIPEDA provides for the handling of personal data, whether domestic or foreign, and has no provisions for cross-border transfers per se.
- Therefore, while cross-border data transfer is generally permitted, the general provisions on transfers of personal data set forth in PIPEDA also apply in the event of a cross-border transfer.
- The principles for the protection of personal data are set forth in PIPEDA Schedule 1, Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96.

<The principles for the protection of personal information>

#### ① Accountability

- Designation of a privacy officer to monitor compliance with the principles
- Ensuring and providing an equivalent level of protection through contracts or other means for third party processing
- Establishing procedures for the protection/implementation of personal data

#### ② Identifying Purposes

- Identification and clarification of the purposes for data collection
- Notification of purpose (re-notification and consent required for use of information for purposes other than those specified)

#### ③ Consent

- Obtaining the data subject's "knowledge and consent"
- Prohibit obtaining consent to the collection, use, or disclosure of personal information as a condition of providing a product or service

#### ④ Limiting Collection

- Limit the collection to the extent necessary for the organization's purposes
- Collecting personal information through appropriate and lawful means

#### ⑤ Limiting Use, Disclosure, and Retention

- Prohibit the use/disclosure for purposes other than those for which it was collected (except with the consent of the individual or as required by law)
- Destruction, deletion/anonymization that is no longer needed

#### ⑥ Accuracy

- Maintain accurate/complete/up-to-date to the extent necessary for the purpose of use

#### ⑦ Safeguards

- Implementation of security safeguards appropriate to the sensitivity of the data (including physical, organizational and technical measures)





# Countries/Regions without related regulations (2/3)

## Canada

### (Continued) Cross-Border Data Transfer Regulations

- ⑧ Openness
  - Ensuring easy access to information about policies/practices for the management of personal data
- ⑨ Individual Access
  - Individuals' access to data, requests for correction of information, and the organization's responsibility to respond to such requests
- ⑩ Challenging Compliance
  - Establishment of a compliance officer to deal with issues related to compliance with the principles
  - Establishment of grievance procedures

In Canada, personal data protection has long been governed by individual/sectoral laws<sup>1</sup>, with a comprehensive private sector personal data protection law finally passed by PIPEDA in 2000. Therefore, the model code CAN/CSA-Q830-96 preceded the law. So, when developing a comprehensive law, Canada adopted a special method of incorporating CAN/CSA-Q830-96 into the comprehensive law.

### Data Localization Regulations

#### Applicable Regulation

No applicable regulation

## Taiwan

### Cross-Border Data Transfer Regulations

#### Applicable Regulation

Personal Data Protection Act (PDPA)  
- Enforced in 2016

#### Target Data

Any information that may be used to directly or indirectly identify a natural person: a natural person's name, date of birth, etc. (Article 2(1))

#### Regulated Persons

A natural person, legal person or group other than those stated in the preceding subparagraph (Article 2(8))

#### Cross-Border Data Transfer Requirements

Cross-border data transfer allowed in general, but authorities may impose restriction on transfers under the following situations (Article 21)

- ① Major national interests are involved
- ② An international treaty or agreement so stipulates
- ③ The country receiving the personal data lacks proper regulations on protection of the data and the data subjects' rights/interests may consequently be harmed
- ④ The cross-border transfer of the personal data to a third country/territory is carried out to circumvent the PDPA

### Data Localization Regulations

#### Applicable Regulation

No applicable regulation

1. If a state has a state law deemed "substantially similar" to PIPEDA, the state law is allowed to apply instead of PIPEDA. As of May 2020, three states' private sector privacy laws and four states' state laws on health information are deemed "substantially similar" (Office of the Privacy Commissioner of Canada "Provincial laws that may apply instead of PIPEDA")

Source: Government of Canada "Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96"; Office of the Privacy Commissioner of Canada "Guidelines for processing personal data across borders"; Personal Data Protection Act





## Countries/Regions without related regulations (3/3)



### United States

#### Cross-Border Data Transfer Regulations

---

Applicable Regulation

No applicable regulation

#### Data Localization Regulations

---

Applicable Regulation

No applicable regulation



### Philippines

#### Cross-Border Data Transfer Regulations

---

Applicable Regulation

No applicable regulation

#### Data Localization Regulations

---

Applicable Regulation

No applicable regulation





## Details of the Results: International Rules

We provide the following details on the next page

		Title	Countries/Regions	Year Issued
Regulation		1 Cross-border transfer/localization regulations in major countries/regions	22 countries/Regions	—
International Rule		1 OECD Guidelines governing the protection of privacy and transborder flows of personal data (OECD Privacy Guidelines)	OECD Members	1980 (revised in 2013)
		2 Convention for the protection of individuals with regards to automatic processing of personal data (Council of Europe Convention 108)	55 countries (Council of Europe 46 countries, and other 9 countries)	1985 (revised in 1999)
		3 APEC Privacy Framework	APEC Members	2004 (revised in 2016)
		4 ASEAN Framework on Personal Data Protection (ASEAN PDP Framework)	ASEAN Members	2016
Trade Agreement		1 General Agreement on Trade in Services (GATS)	WTO Members	1995
		2 Regional Trade Agreement (FTA)		
		i) Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)	Japan, Singapore, Vietnam, Australia, New Zealand, Canada, Mexico	2021
		ii) Regional Comprehensive Economic Partnership Agreement (RCEP)	ASEAN Members (10 countries), Japan, South Korea, China, Australia, New Zealand	2022





# 1 OECD Privacy Guidelines (1/2)

## Basic Policies

The OECD requires its members to implement the OECD Privacy Guidelines, which set forth the protection of privacy in general, not just in the context of cross-border transfer. The eight core OECD Privacy Principles do not include specific reference to cross-border transfers, but they apply as principles for the handling of personal data that should naturally be followed in the event of a cross-border transfer.

## Background

Growing concerns about personal data with the advent of computers since the 1960s sparked a worldwide data protection debate, and in the 1970s, some developed countries enacted privacy laws.

In response to these growing discussions on data protection, the OECD adopted the former OECD Privacy Guidelines (Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data) in 1980. In this document, the OECD established eight privacy principles and required member countries to "consider privacy in national laws," "not unreasonably impede the international flow of personal data under the guise of privacy protection," and "cooperate in implementing the guidelines," which have come to be used as de facto global standards.

Subsequently, with the spread of the Internet, the network society progressed rapidly. In response to the transformation of personal data protection issues, and in light of "changing technologies, markets and user behavior, and the increasing importance of digital identities," the OECD began discussions on revising the Guidelines. On the occasion of the 30th anniversary of the enactment of the Guidelines, full-fledged discussions on the revision were initiated, and the revised version was adopted in 2013.

## Details

### Target

Public and private sectors (all stakeholders)

### OECD Privacy 8 Principles

#### 1) Collection Limitation Principle

Limitations must be placed on the collection of personal data, and any personal data must be collected by lawful and fair means, with notice to and consent of the data subject.

#### 2) Data Quality Principle

Personal data must be used within the scope of the purpose and must be accurate, complete, and up-to-date to the extent necessary to achieve that purpose.

#### 3) Purpose Specification Principle

The purpose for which personal data is collected must be specified prior to collection, and subsequent uses must be limited to the extent necessary to achieve the purpose. In addition, the purpose of any other use must be specified each time it is used.

#### 4) Use Limitation Principle

Personal data shall not be provided except with the consent of the data subject or with legal authorization.

#### 5) Security Safeguard Principle

Personal data shall not be provided except with the consent of the data subject or with legal authorization.





# 1 OECD Privacy Guidelines (2/2)

(continued) OECD Privacy 8 Principles

## 6) Openness Principle

There must be a publicly available general policy regarding personal data utilization, handling, practices and policies. It must also indicate the existence and nature of the personal data, the purposes for which it is to be used, and the data controller and its location

## 7) Individual Participation Principle

Individuals have the right to obtain confirmation as to whether a data controller is in possession of their personal data. They also have the right to demand that the controller communicate such data to them within a reasonable period of time, at a reasonable cost, if necessary, and in a reasonable and recognizable manner. If such a request is refused, the data subject shall have the right to demand that the controller explain the reasons for the refusal and to object to the reasonableness of the refusal. If the objection is accepted, the data concerned may be erased, corrected or perfected.

## 8) Accountability Principle

The data controller is responsible for complying with measures to implement each principle





## 2 Council of Europe Convention 108 (1/2)

### Basic Policy

Led by the Council of Europe, the Council of Europe Convention No. 108 exists as the regulation governing privacy protection. It is ranked as one of the oldest legally binding personal data protection frameworks and refers early on to cross-border transfers, including a general prohibition on restrictions on cross-border transfers between signatory countries.

### Background

In the 1970s, Europe actively debated the protection of personal data with reference to Article 8 of the European Convention on Human Rights (1953). The OECD and four non-member countries (the United States, Japan, Canada, and Australia) participated as observers in the discussions, which culminated in the signing of Council of Europe Convention No. 108 in 1981, which entered into force in 1985.

Council of Europe Convention No. 108 is the only binding international instrument in the field of data protection and was amended in 1999 in conjunction with the Lisbon Treaty and adopted as an Additional Protocol in 2001 (Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows).

As of September 2022, a total of 55 countries (46 members and 9 non-members) have ratified the Convention, and discussions on its further modernization have been underway in recent years.

### Details

#### Definition of "Cross-border data transfer"

The transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed (Article 12(1))

#### Target Data

Convention 108 defines the scope of application of the Convention as follows (Article 3(1)). And article 12(1) states that the same data is also covered by the Convention with respect to cross-border transfers).

- Automated personal data files and automatic processing of personal data in the public and private sectors.

#### Detail of Convention 108

Convention 108 prohibits in principle restrictions on cross-border transfers to other Contracting Parties for the sole purpose of protecting personal data.

However, exceptions to the restrictions on transfers may be made if any of the following conditions are met.

- ① Specific Regulations (Article 12(3)a)  
Insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection
- ② The transfer to a non-Contracting State (Article 12(3)b)  
When transfers are made from a Contracting State to a non-Contracting State through the intermediary of another Contracting State, restrictions on transfers are permitted in order to prevent such transfers from circumventing the laws of the Contracting State.





## 2 Council of Europe Convention 108 (2/2)

### Detail of Additional Protocol

Additional Protocol Article 2 provides, with respect to the cross-border transfer of personal data to recipients not within the jurisdiction of a Contracting State

- ① Transfer to a country/agency outside of the treaty jurisdiction with an adequate level of protection (Article 2(1))

Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organization that is not Party to the Convention only if that State or organization ensures an adequate level of protection for the intended data transfer.

- ② Exceptions (Article 2(2))

By way of derogation, each Party may allow for the transfer of personal data:

- a. If domestic law provides for it because of:
  - Specific interests of the data subject
  - Legitimate prevailing interests, especially important public interests
- b. If safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.





### 3 APEC Privacy Framework (1/2)

#### Basic Policy

APEC recommends that member countries implement the APEC Privacy Framework. It generally follows the OECD Privacy Guidelines and requires reasonable measures to obtain the consent of the individual and ensure compliance with the principles with respect to cross-border transfers.

#### Background

APEC began discussions on personal data protection starting with an agreement at the 1998 Ministerial Meeting, which led to the formulation and approval of the APEC Privacy Framework in 2004. In recent years, APEC has also focused on the cross-border transfer of personal data, particularly within the APEC region, and in 2011 began operating the CBPR System (APEC Cross Border Privacy Rules System). The APEC Privacy Framework itself was updated in 2016 (Revised APEC Privacy Framework) to include provisions on cross-border transfers.

#### Details

##### Target Data

Any information about an identified or identifiable individual (Article 9)

##### Regulated Person

Personal information controller (Article 10)

A person or organization who controls the collection, holding, processing or use of personal information. It includes a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf but excludes a person or organization who performs such functions as instructed by another person or organization. (Article 10)

#### APEC Information Privacy Principles

##### 1) Preventing Harm (Article 14)

Specific obligations should take into account the risks created by the misuse of personal data, and remedies should be proportionate to the likelihood and severity of harm from the collection, use, and transfer of information.

##### 2) Notice (Article 15-17)

Personal information controllers must provide, in an accessible manner, the facts of the collection of personal data, its purpose, the types of third parties to whom it is disclosed, the name and location of the personal data controller, and the policies and systems regarding personal data, including limitations on the use and provision of personal data and methods for disclosure and correction.

##### 3) Collection Limitation (Article 18)

Personal data must be collected within the scope of the purpose and by lawful and fair means.

##### 4) Use of Personal Information (Article 19)

In principle, the use of personal data shall be limited to the fulfillment of the purpose for which it was collected and related purposes. Exceptions may be made (i) where the data subject has given consent, (ii) where it is necessary to provide services or products requested by the data subject, or (iii) where required by law.

##### 5) Choice (Article 20)

Clear, easily understood and accessible mechanisms must be provided for individuals to exercise their choices regarding the collection, use and disclosure of their personal data.

##### 6) Integrity of Personal Information (Article 21)

To the extent necessary for the purpose of use, personal data must be accurate, complete, and current.





## 3 APEC Privacy Framework (2/2)

(continued) APEC Information Privacy Principles

### 7) Security Safeguards (Article 22)

Personal Data Controllers must protect personal data appropriately by maintaining appropriate safeguards against risks such as loss, unauthorized access or destruction, use, alteration, and disclosure of personal data.

### 8) Access and Correction (Article 23-25)

Individuals may verify data retained by the personal data controller. After satisfactory identification, individuals may receive communication of their personal data in a reasonable manner. If there is any doubt as to the accuracy of the information, the individual may request correction, deletion, etc., and if the request is denied, may request disclosure of the reasons for the denial.

### 9) Accountability (Article 26)

The personal data controller is responsible for realizing the above principles. When transferring personal data, whether domestically or internationally, the consent of the individual must be obtained, or reasonable steps taken to ensure that the recipient provides the same level of protection as the above principles.

Additional provisions on cross-border data transfer in the revised version

- ① Avoiding Restrictions on Cross-Border Transfer to Other Members (Article 69)  
A member economy shall avoid restrictions on cross-border transfers if:
  - The transferring country has introduced legislation or other measures to implement the relevant framework
  - Adequate safeguards exist to implement such a framework, including enforcement mechanisms and appropriate measures (e.g., CBPR) implemented by the controller of personal data.
- ② Risk Proportionate Restrictions on Cross-Border Transfers (Article 70)  
Any restrictions on cross-border transfers must be proportionate to the risks assumed. In considering the risks, the sensitivity of the information, the purpose and circumstances of the transfer must be taken into account.





## 4 ASEAN PDP Framework (1/2)

### Basic Policy

ASEAN encourages member countries to implement in their national laws the basic principles regarding personal data set forth in the ASEAN PDP Framework. The principles themselves are similar to the preceding OECD Privacy Guidelines and the APEC Privacy Framework. With respect to cross-border transfers, the Principles also require notification of cross-border transfers, prior consent of the individual concerned, and the implementation of measures to ensure the level of protection of personal data required by the Principles.

### Background

ASEAN, which aims to cooperate on economic growth and various issues in the Southeast Asian region, adopted the ASEAN PDP Framework in 2016, building on the preceding OECD Privacy Guidelines and APEC Privacy Framework. Like the two preceding principles, the ASEAN PDP Framework establishes basic principles for personal data protection and encourages member states to implement the principles in their national laws. After the adoption of the PDP Framework, ASEAN has continued its activities to promote data distribution and growth in the region, including the establishment of the ASEAN Model Clause.

### Details

#### Target Data

The aim is to "strengthen the protection of personal data in ASEAN" (Article 1), but no mention of the specifics of "personal data."

#### Regulated Person

This Framework will not apply to (Article 4):

- Measures adopted by a Participant to exempt any areas, persons or sectors from the application of the Principles
- Matters relating to national sovereignty, national security, public safety, public policy and all government activities deemed suitable by a Participant to be exempted.

#### Framework on Personal Data Protection

##### 1) Consent, Notification, and Purpose (Article 6a/b)

- An organization should not collect, use or disclose personal data about an individual unless:
  - The individual has been notified of and given consent to the purpose(s) of the collection, use or disclosure of his/her personal data
  - The collection, use or disclosure without notification or consent is authorized or required under domestic laws and regulations.
- An organization may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances.

##### 2) Accuracy of Personal Data (Article 6c)

The personal data should be accurate and complete to the extent necessary for the purpose(s) for which the personal data is to be used or disclosed.

##### 3) Security Safeguards, 6d)

The personal data should be appropriately protected against loss and unauthorized access, collection, use, disclosure, copying, modification, destruction or similar risks.





## 4 ASEAN PDP Framework (2/2)

(continued) Framework on Personal Data Protection

### 4) Access and Correction (Article 6e)

Upon request by an individual, an organization should:

- Provide the individual access to his/her personal data which is in the possession or under the control of the organization within a reasonable period of time.
- Correction of errors or deficiencies in personal data (not limited to cases where there are provisions under domestic laws, etc.)

### 5) Transfers to Another Country or Territory (Article 6f)

In the event of a cross-border transfer, prior consent for the cross-border transfer must be obtained, and reasonable measures must be taken to ensure that the transferee has the same level of personal data protection as the principle in question.

### 6) Retention (Article 6g)

The organization must retain documents containing personal data or discontinue or delete the means of personal identification when the retention of the data is no longer necessary for legal or business purposes.

### 7) Accountability (Article 6h/i)

- An organization should be accountable for complying with measures which give effect to the Principles.
  - An organization should, on request, provide clear and easily accessible information about its data protection policies and practices with respect to personal data in its possession or under its control.
    - An organization should also make available information on how to contact the organization about its data protection policies and practices.
- Implementation.





# Details of the Results: Trade Agreement

We provide the following details on the next page

		Title	Countries/Regions	Year Issued
Regulation		1 Cross-border transfer/localization regulations in major countries/regions	22 countries/Regions	—
International Rule		1 OECD Guidelines governing the protection of privacy and transborder flows of personal data (OECD Privacy Guidelines)	OECD Members	1980 (revised in 2013)
		2 Convention for the protection of individuals with regards to automatic processing of personal data (Council of Europe Convention 108)	55 countries (Council of Europe 46 countries, and other 9 countries)	1985 (revised in 1999)
		3 APEC Privacy Framework	APEC Members	2004 (revised in 2016)
		4 ASEAN Framework on Personal Data Protection (ASEAN PDP Framework)	ASEAN Members	2016
Trade Agreement		1 General Agreement on Trade in Services (GATS)	WTO Members	1995
		2 Regional Trade Agreement (FTA)		
		i) Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) ii) Regional Comprehensive Economic Partnership Agreement (RCEP)	Japan, Singapore, Vietnam, Australia, New Zealand, Canada, Mexico ASEAN Members (10 countries), Japan, South Korea, China, Australia, New Zealand	2021 2022





# 1 GATS (1/2)

## Basic Policy

The GATS applies to WTO members, and while it is not primarily focused on the protection of personal data, it can be relevant because data distribution is often part of the provision of some type of service

Due to the different primary focus, there is no direct mention of restrictions or permissions on cross-border transfers but depending on the nature of the cross-border transfer restrictions, it may be a violation of the obligations set forth in the GATS

## Background

GATS was issued in 1995 as part of the WTO Agreement.

The WTO Agreement includes the Agreement Establishing the World Trade Organization (Marrakesh Agreement) and Annexes 1-4. WTO membership requires collective acceptance of Annexes 1-3, including the Agreement Establishing the WTO and GATS (Annex 1B), and therefore, all WTO members are subject to GATS

## Details

### Scope

- The GATS allows each member country to choose to accept obligations under the GATS in each of the 12 service areas defined in the Table of Commitments, with the exception of some obligations
- For data distribution, Computer and Related Services and Telecommunications Services are relevant

### Regulated Person

WTO Members

## Relationship between obligations under GATS and data distribution

The four GATS obligations related to data distribution are:

### 1) Most-Favoured-Nation Treatment (Article 2)

The most favorable treatment accorded to any one of the countries shall be accorded to all members. (Note that the most-favored-nation treatment shall be applied uniformly to all member countries, with no choice allowed to each member country)

- Therefore, imposing non-uniform co-creation conditions on services and service providers in other Member States, e.g., through cross-border transfer restrictions, may result in a possible violation of this obligation

### 2) Obligation to reasonably enforce domestic regulations (Article 6)

Member States shall ensure that any generally applicable Member State measures affecting trade in services in the services sectors in which they have committed to liberalize are implemented in a reasonable, objective and impartial manner

- Therefore, if a Member State applies cross-border restrictions, etc. in an unreasonable manner to services and service providers in another Member State, the issue of a breach of this obligation may arise

### 3) Market Access Obligation (Article 16)

Member States shall not restrict the number of service providers or the total volume of services in service sectors to which they have committed to market access

- The introduction of restrictions on cross-border transfers of online data processing or database services may be considered as a restriction on the number of service providers





# 1 GATS (2/2)

(continued) Relationship between obligations under GATS and data distribution

## 4) National Treatment Obligation (Article 17)

The services and service providers of other Member States shall be treated no less favorably than national services and service providers of the same type.

- As with the MFN obligation, a possible violation of this obligation may arise depending on the content of cross-border transfer regulations, etc. In particular, the national storage obligation requires the establishment of servers, etc. within a member country, which imposes additional burdens on service providers in other member countries, and thus may result in a violation of this obligation

## Exceptions to the GATS Obligation

A violation of the GATS obligation is justified if the following exceptions are met

### ① General Exceptions (Article 14)

Measures necessary for the maintenance of public order and the protection of life or health, etc.

### ② Security Exceptions (Article 14 bis)





## 2 RTA (1 / 2)

### CPTPP

#### Background and Relevance to Regulations on Cross-Border Data Transfer

The CPTPP entered into force in 2021 with the aim of liberalizing not only tariffs on goods but also services and investment in the Pacific Rim, as well as establishing rules in a wide range of areas, including intellectual property and e-commerce.

Like the GATS, the agreement does not focus primarily on cross-border transfers, but it does mention data distribution, including personal data, in its provisions on e-commerce.

#### Target Data

- Unless otherwise stated, information in general is subject to regulation
- However, references to "personal information" mean "any information, including data, about an identified or identifiable natural person" (Chapter 14 Article 1)

#### Regulated Person

- The subject of the regulation is unambiguously a Contracting State
- The "covered persons" referred to in the rules covering cross-border transfers (Chapter 14, Article 11) refer to "covered investment property," "investors of a Contracting State" and "service providers of a Contracting State" (financial institutions and providers of financial services are excluded) (Chapter 14, Article 1)

#### Details

- Article 11 of Chapter 14 provides for the cross-border transfer of information and, in principle, prohibits the regulation of cross-border transfers
  - Parties shall permit the cross-border transfer of information (including personal data) by electronic means if it is carried out for the conduct of the subject's business (Chapter 14, Article 11(2))
- Exceptions to the regulation are permitted in the following cases:
  - Where necessary for a Contracting State to achieve a legitimate public policy objective (Chapter 14, Article 11(3))
  - The case falls within the scope of GATS Article 14a-c (general exceptions) (Chapter 29, Article 1(3))the case falls under the exception for security reasons (Chapter 29, Article 2)





## 2 RTA (2/2)

### RCEP

#### Background and Relevance to Regulations on Cross-Border Data Transfer

The RCEP entered into force in 2022 with the aim of promoting trade and investment in the signatory countries and regions, improving market access for more efficient supply chains, and establishing rules in a wide range of areas such as intellectual property and e-commerce among the signatory countries. Like other trade agreements such as GATS and CPTPP, it does not focus primarily on cross-border transfers, but it does mention data distribution, including personal data, in its e-commerce provisions.

#### Target Data

- Unless otherwise stated, information in general is subject to regulation
- However, references to "personal information" mean "any information, including data, about an identified or identifiable natural person" (Chapter 1, Article 1.2u)

#### Regulated Person

- The subject of the regulation is unambiguously a Contracting State
- In addition, "covered persons" referred to in the rules covering cross-border transfers (Chapter 12, Article 15) refer to "covered investment property," "investors of a Contracting State" and "service providers of a Contracting State" (financial institutions and providers of financial services are excluded) (Chapter 12, Article 1).

#### Details

- Like the CPTPP, RCEP also prohibits in principle the regulation of cross-border transfers (Chapter 12, Article 15)
  - Contracting States shall not prevent the cross-border transfer of information by electronic means if such transfers are made for the conduct of the business of the subject (Chapter 12, Article 15, Paragraph 2)
- Exceptions to the regulation may be made, however, in the following cases:
  - Where a Contracting State deems it necessary to achieve a legitimate objective of public policy, the Contracting State considers it necessary in order to achieve legitimate objectives of public policy, provided that such measures are not applied in such a manner as to constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade (Chapter XII, Article 15, paragraph 3(a))
  - Where a Contracting State considers it necessary for the protection of its vital interests of security (Chapter XII, Article 15, paragraph 3b)










## 2.3

# Details of the Results: Cross-Border Data Transfer Tools



# Cross-Border Data Transfer Tools

Focus on cross-border transfer tools used in the target countries/regions (5/12 are not included in the detailed survey)

		Title	Scope	Registration based on	Start with
By Country 	Certification 	① Adequacy Decision/Whitelist	EU/UK → Outside Japan → Outside Russia → Outside Turkey → Outside Vietnam → Outside Brazil → Outside Thailand → Outside	GDPR/UK GDPR APPI 152-FZ DPL Draft on the protection of data LGPD PDPA	2016- 2005- 2006 No Operational Track Not Implemented (Details undecided) Not Implemented (Details undecided) <sup>1</sup> Not Implemented (Details undecided) <sup>1</sup>
		② Japan-EU Supplementary Rules	EU → Japan	GDPR	2018-
		③ Trans-Atlantic Data Privacy Framework (TADPF)	EU ↔ US	GDPR	Not Implemented (Agreed in principle)
		④ Standard/Model Contractual Clauses (SCC/MCC)	EU/UK → Outside China → Outside NZ → Outside Within ASEAN Within Ibero-America Singapore → Outside Brazil → Outside	GDPR/UK GDPR PIPL Privacy Act ASEAN PDP Framework RIPD PDPR LGPD	1995- Not Implemented (Opinions collected) 2020- 2022 2021- 2022- Not Implemented (Details undecided) <sup>1</sup>
		⑤ Other contracts, etc.	Many	Many	—
		⑥ Binding Corporate Rules (BCR)	EU/UK → Outside Singapore → Outside Brazil → Outside	EU/UK GDPR PDPR LGPD	2016- 2021- Not Implemented
		⑦ Outbound Data Transfer Security Assessment	China → Outside	PIPL	2022-
		⑧ Certification of Personal Information Cross-Border Processing Activities	China → Outside	PIPL	Not Implemented (Details undecided) <sup>1</sup>
By Business 	Contract 	⑨ Cross Border Privacy Rules (CBPR)	9 Member Countries	APEC Privacy Framework	2011-
		⑩ APEC Privacy Recognition for Processors (APEC PRP)	Within APEC	APEC Privacy Framework	2015-
		⑪ Codes of Conduct (CoC)	EU/UK → Outside Brazil → Outside	EU/UK GDPR LGPD	2016- Not Implemented (Details undecided) <sup>1</sup>
		⑫ Consent of the data subject	Many	Many	—
	Certification 				
	CoC				
	Others				

1. The regulation is enforced already, but the tool has not implemented.



## Summary of the results (1/4)

The hurdles for countries/regions to operate cross-border transfer tools are high, and only a few countries/regions are actually able to do so



Various cross-border transfer tools, including multi-country tools, exist as data distribution becomes more active.

- Like regulations, each country/region has developed its own tools similar or identical to those specified in the GDPR (adequacy decision, SCC/MCC, BCR, Codes of Conduct, etc.)
- Cross-border data transfer tools are also being developed at the regional level, such as APEC and Ibero-America, but in the case of tools that can be used in multiple countries/regions, some of them are less comprehensive than those defined at the single country/region level (e.g., ASEAN MCCs).



The SCC/MCC, which organizes and publishes the requirements necessary to achieve cross-border data transfer as a template, is highly convenient, and it is the tool most countries/regions have adopted as of September 2022.

- China has also published SCC, and even countries that are promoting localization cannot ignore the need to deal with cross-border transfers.
- Furthermore, SCC/MCC is recognized as a highly convenient tool regardless of the attitude toward data distribution in each country/region.



Many countries/regions, such as Brazil and Singapore, have prescribed tools similar to those in the EU, but the hurdles for operating the tools are high, so there are not many operational results in non-EU countries/regions as of September 2022.

- Brazil has developed regulations and adopted tools similar to GDPR, but none of the tools are actually operational
- Singapore has also adopted tools similar to GDPR, but by proactively incorporating tools regulated at the regional level, it is reducing operational costs and ensuring the convenience of cross-border data transfer.



# Summary of the results (2/4): Comparison of Cross-Border Transfer Requirements

There are differences in requirements depending on the purpose of each tool/parties, and in the coverage of the basic privacy principles

			④ SCC/MCC ※Controller-Controller								⑥ BCR			Other Certifications						⑪ CoC	
			② Japan-EU Rules	EU	UK	China	Ibero-America	NZ	ASEAN	Singapore	EU	UK	Singapore	⑦ China Sec. Assessment	⑧ China Cert. of Transfer	⑨ CBPR	⑩ PRP	EU	UK		
Obligations of the Parties	Privacy Principles	Processing Limitation	●	●	●	●	●	●	●	Recommends use of ASEAN MCCs  Minor modifications are necessary	●	●	Requires clear specification of rights and obligations	●	●	●	●	●	●		
		Notification		●	●	●	●		●		3	3		●	●	●	●	●	●	●	
		Accuracy		●	●		●	●	●		●	●		●	●	●	●	●	●	●	
		Security Safeguards		●	●	●	●	●	●		●	●		●	●	●	●	●	●	●	●
		Participation/Access		●	●	●	●	●			●	3		3	No individual designation of rights and obligations to be clearly stated	●	●	●	8	8	
		Harm Prevention																			
	Others	Accountability		●	●	●	●	●	2	●	●	3	3	●	●	●	5	5			
		Restrictions for Sensitive Data	●	●		1	●	●			●	●	●	●	●	●	●		●	●	
		Third Party Use	●	●	●	●	●			●	●	●	●	●	●	●	●		●	●	
		Details of Implementation		●	●	●	●	●	●	●	●	●	●	●	●	●	●				
Rights of the Data Subject			●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●		
Personal Data Breach Handling			●	●	●	●	●	●	●	●	●	●	●	●	●	●	6	●	●		
Dispute Resolution			●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●		
Request for Disclosure by Public Authorities			●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●		
Third Country Law Impact Assessment			●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●		
Supervision			●	●	●	●	●		●	●	●	●	●	●	●	●		●	●		
			●					●		●	●	●	●	●	●	●		●	●		
											●	●				7	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				
											●	●				●	●				

1. China SCC only requires notification of the need for the transfer and the impact of the transfer on the data subject but does not require restrictions on handling or implementation of additional safeguards (Article 2.2) 2. no clear performance responsibility/compliance statement but does specify that a person responsible for monitoring compliance with the contract (NZ MCC General Clause Article 1.7) (NZ MCC General Clause Article1(7)) 3. requires "application of general data protection principles" (GDPR/UK GDPR Article 47(2)d) 4. requires the establishment of a privacy officer and a personal data protection organization (China Certification of Cross-Border Activities Article4(2)) 5. require "1.1 Compliance with privacy principles" (CBPR Standard) 6. require "1.7 Emergency situation" item etc. to respond to a breach (CBPR Standard) 7. list personal data protection officers in the roles to be prepared (CBPR Standard 8.1) 8. although not mentioned, it is assumed that the right of access is included in the "exercise of data subjects' rights" (since the right of access is generally recognized as a data subject right under EU/UK law)



# Summary of the results (3/4): Comparison of Security Safeguards Requirements<sup>1</sup>

Each country provides a level of personal data protection, including transfers, but there are differences

● :Applicable

	4 SCC/MCC							6 BCR			Other Certifications				11 CoC	
	EU	UK	China	Ibero-America	NZ	ASEAN	Singapore	EU	UK	Singapore	7 China Sec. Assessment	8 China Cert. of Transfer	9 CBPR	10 PRP	EU	UK
Pseudonymization and encryption	●		●	●	Not Specified	Not Specified	Recommends use of ASEAN MCCs	Not Specified		Require specification of rights and obligations	Not Specified	Not Specified		●	●	●
Ensuring confidentiality, integrity, availability	●			●	Not Specified	Not Specified	Recommends use of ASEAN MCCs	Not Specified		Require specification of rights and obligations	Not Specified	Not Specified			●	●
Ensuring data availability and restoration of access in event of incident	●			●	Only require implementation and maintenance of "worldwide /generally expected standards of business" safeguards <sup>4</sup>	Only requires appropriate security measures in accordance with AMS law or as agreed to by the parties <sup>5</sup>	Minor modifications are necessary.	Only requires "data security" <sup>6</sup>		No individual designation of rights and obligations to be clearly stated	Only requires "administrative and technical measures to fulfill liability obligations and the ability to ensure the security of cross-border data." <sup>7</sup>	Only require "necessary measures to comply with the personal data protection standards set forth in the relevant laws and regulations <sup>8</sup>	●	●	●	●
Regular testing to ensure security of processing	●		●	●									●	●	●	●
User identification and authorization	●			●									●	●		
Protection of data during transfer	●	●		●									●		●	●
Protection of data during storage	●	●		●									●		●	●
Ensuring physical security of locations where personal data is processed	●			●									●			
Ensuring event logging	●			●									●	●		
Ensuring system configuration	●			●												
Internal IT and IT security governance and management	●		●	●									●	●	●	
Assurance/certification of processes/products	●			●										●		
Data minimization	●			●											●	
Data quality	●			●												
Limited data retention	●			●												
Accountability	●			●											●	
Data portability	●															
Others		Few specific enumerations, only summary level enumerations <sup>2</sup>	Few specific enumerations, only summary level enumerations <sup>3</sup>													

1. Since the wording differs depending on the tool, it is described here as "security protection measures" and compared based on the technical and organizational measures of EU SCC Annex II.

2. In Table 4 of Part 1 of [IDTA](#), there are only descriptions of Organizational Security Measures, Technical Security Measures, Security of Transmission, and Security of Processing. No specific method (e.g., encryption) is specified. 3. [China SCC](#) Article 2.4 only mentions "technical and administrative measures such as encryption, anonymization, de-identification, access control, etc." 4. [NZ MCC](#) Part 2 General Provisions Article 1.3 5. [ASEAN MCCs](#) Article 3(2) 6. [GDPR](#) Article 47(2)d, [UK GDPR](#) Article 47(2)d 7. [Cyber Security Law](#) Article 5(3) 8. [China Certification of Cross-Border Activities](#) Article 3d



## Summary of the Results (4/4): Comparison of Major Cross-Border Transfer Tools

	SCC/MCC	BCR	CBPR
Country	EU, UK, Singapore, China, New Zealand, Brazil <sup>1</sup> , ASEAN, Ibero-America	EU, UK, Singapore, Brazil <sup>1</sup>	Japan, US, Canada <sup>2</sup> , Mexico <sup>2</sup> , Singapore, South Korea, Australia <sup>2</sup> , Taiwan, Phillipine <sup>2</sup>
Type	Contract	Internal Policy	Certification
Model Format	Available	NOT Available	NOT Available
Approval	NOT required	Required	Required
Concreteness of Requirements	Concrete <ul style="list-style-type: none"> <li>- Published in a model format with concrete requirements</li> </ul>	NOT concrete <ul style="list-style-type: none"> <li>- Requirements provide an overview. Companies are free to interpret it.</li> </ul>	Concrete <ul style="list-style-type: none"> <li>- Agency provides concrete requirements</li> </ul>
Differences b/w Countries	NOT significant	Significant	None
Cost	Middle <ul style="list-style-type: none"> <li>- Requirements are specifically enumerated, so it is easy to use</li> <li>- Companies need multiple contracts when transferring data with this tool (high cost)</li> </ul>	High <ul style="list-style-type: none"> <li>- Companies are free to consider details by themselves (need lots of time/human resources)</li> </ul>	Low <ul style="list-style-type: none"> <li>- Companies should establish the required internal data protection system, but the requirements are common to other data protection certifications</li> </ul>
Applicable Area	Wide <ul style="list-style-type: none"> <li>- Adopted by many countries</li> </ul>	Narrow <ul style="list-style-type: none"> <li>- Adopted by few countries</li> </ul>	Narrow <ul style="list-style-type: none"> <li>- Adopted by few countries</li> </ul>

1. The regulation stipulates SCC/MCC and BCR as requirements for allowing cross-border transfers, but the details have not yet been determined, 2. Actual operation has not yet started due to the lack of an accountability agency, 3. The requirements do not require the detailed internal operational structure, but the final draft seems to include it (e.g., petition procedures, etc.).





# 1 Adequacy Decision (1/2)

## Overview

Adequacy decision is one of the requirements for the cross-border transfer of personal data stipulated in the GDPR. In addition to the GDPR, seven other countries, including the U.K. and Japan, have adopted a similar mechanism, but the EU is the only region in which it is practically operational as of September 2022, as it requires the establishment of an authorization agency and the development of a certification system, etc.

## Adequacy Decision in EU GDPR

### Justification Basis

GDPR Article 45

### Subject of Certification

Third country, third national region or sector of characteristics (including multiple sectors), international organization.

### Authorization Agency

European Commission

## Requirements

The Commission shall assess the level of data protection taking into account the following (Article 45(2))

- The situation in third countries with regard to legislation, case law, administrative and judicial remedies available to data subjects, including the rule of law, respect for human rights and fundamental grounds, public safety, national security, etc.
- The existence of a supervisory authority with appropriate enforcement powers and the effective functioning of that authority.
- Conventions, etc. to which third countries are parties regarding the protection of personal data.

## Procedures

1. Proposal from the European Commission
2. Opinion by the European Data Protection Board (EDPB)
3. Approval by EU Member State representatives
4. Adoption of the decision by the European Commission (=approval)

## Renewal and Cancellation

- The Commission shall review accreditation at least every four years (Article 45(3)).
- If the Commission finds that the object of accreditation does not ensure an adequate level of protection, it shall withdraw, modify or suspend the accreditation to the extent necessary (Article 45(5)).





# 1 Adequacy Decision (2/2)

## Approval Status

● :Adequate countries

	EU	UK	Japan	Russia	Turkey	Vietnam	Brazil	Thailand
1 EU/EEA Countries		●	●	●	N/A	N/A Just Draft	N/A	N/A Implementing rules not yet established
2 Azerbaijan				●				
3 Argentina	●	●		●				
4 Albania	●			●				
5 Armenia	●			●				
6 Andorra	●	●		●				
7 United Kingdom	●		●	●				
8 Ukraine	●			●				
9 Uruguay	●	●		●				
10 Cape Verde	●			●				
11 North Macedonia	●			●				
12 Georgia	●			●				
13 San Marino	●			●				
14 Switzerland	●	●		●				
15 Senegal	●			●				
16 Serbia	●			●				
17 Tunisia	●			●				
18 Turkey	●			●				
19 Bosnia	●			●				
20 Mexico	●			●				
21 Mauritius	●			●				
22 Monaco	●			●				
23 Moldova	●			●				
24 Morocco	●			●				
25 Montenegro	●			●				
26 Israel	●	●						
27 Guernsey	●	●						
28 Jersey	●	●						
29 Isle of Man	●	●						
30 Canada	●	●						
31 South Korea	●							
32 Japan	●	●						
33 New Zealand	●	●						
34 Faroe Islands	●	●						

Source: Created from publicly available information





## 2 Supplementary Rules (JP-EU)

### Overview

Japan and the EU have mutually certified that both have adequate protection of cross-border transfers of personal data based on national/regional regulations. However, compliance of additional rules (Supplementary Rules) is required to ensure a high level of protection for personal data transferred from the EU based on an Adequacy Decision, as there are some differences in the legal systems between Japan and the EU

### Background

EU and Japan adopted Adequacy Decision based on GDPR, and Japan's Personal Data Protection Commission issued "Supplemental Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision" in 2018. It was revised in 2019 after the UK withdrew from the EU.

### Justification Basis

- Japan: Act on the Protection of Personal Information
- GDPR Article 45

### Details

#### Scope of application

Supplementary Rules Preamble defines the scope of application as follows

- Personal data transferred from EU based on an Adequacy Decision
- Personal data transferred from UK (after withdrawal from the EU) based on an Adequacy Decision

#### Targets

Businesses receiving to use personal data transferred from EU/UK based on an Adequacy Decision (Preamble)

### Description

The Supplementary Rules establish the following requirements

1. Special care-required personal information
  - If personal data transferred based on an Adequacy Decision contains special categories of personal data under the GDPR and the UK GDPR (e.g., sexual orientation, businesses handling personal information are required to handle them in the same manner as "special care-required personal information" (APPI Article 2.3)
2. Specifying a utilization purpose, restriction due to a utilization purpose
  - When receiving personal based on an Adequacy Decision, a business handling personal information must confirm and record the circumstances of acquisition, incl the purpose of use, in accordance with APPI Article 30.1&3(the same applies when receiving such data from other business which have received data based on an Adequacy Decision)
  - In any case, when providing personal data, the purpose of use must be specified, and the data must be used within the scope of that purpose
3. Restriction on provision to a third party in a foreign country
  - When providing a third party in a foreign country with personal data provided based on an Adequacy Decision, a business handling personal info is required to obtain the consent of the individual to provide data to the said party in advance, excl cases falling under requirements of APPI Article 28
4. Anonymously processed information
  - Personal data provided based on an Adequacy Decision is considered as anonymously processed info only when a business handling personal info makes it impossible for any person to re-identify the anonymized individual by deleting information such as processing method





### 3 TADPF

#### Overview

TADPF is the latest EU-US framework for the cross-border transfer of personal data. Since the US, which does not have a comprehensive personal data protection law, has had difficulty obtaining EU adequacy decisions, it has been negotiating diplomatically and concluding individual agreements to achieve cross-border transfers of personal data.

The EU and US government have addressed issues including complaints by EU citizens over the use of personal data by global Big Tech, and invalidation of the framework by the European Court of Justice (see right)

#### Background

See right

#### Justification Basis

GDPR Article 45

#### Details

##### Key principles

The latest announcement on TADPF provides the following principles for the cross-border transfer of data between the EU and participating the US companies

- Limited access to data by the US information agencies
- Independent and binding remedy mechanisms, including Data Protection Review Court
- Continuing obligations on companies regarding the processing of transferred personal data
- New monitoring and review mechanisms

##### Next step

Legal documentation of the principles agreed in Ma 2022

- Issuance of US Executive Order incorporating the principles
- Adequacy decision of the Executive Order by the European Commission

#### History of the EU-US cross-border transfer of personal data<sup>1</sup>

- Dec 1995 EU Data Protection Directive enacted
- Jul 2000 Agreed to introduce the Safe Harbor Privacy Principles, a framework for the cross-border transfer of personal data between EU and the US
- Jul 2001 Safe Harbor Privacy Principles enacted
- Jun 2013 Complaint filed by Max Schrems regarding personal data protection
  - Austrian lawyer Max Schrems filed a complaint with the Irish Data Protection Commissioner against Facebook's transfer of personal data to the US, claiming US agencies' monitoring activities do not ensure adequate protection of personal data
- Jun 2013 The Snowden Affair
  - Former CIA employee Edward Snowden exposed the collection of personal information by the National Security Agency
- Jun 2014 Max Schrems complaint referred to the European Court of Justice
- Oct 2015 Safe Harbor Privacy Principles invalidated by the European Court of Justice (Schrems I judgement)
- Feb 2016 Agreed to introduce a new framework, the EU-US Privacy Shield
- Jul 2016 Privacy Shield adopted
- Aug 2016 Privacy Shield enacted
- Dec 2016 European Commission certified sufficiency of Privacy Shield
- May 2018 GDPR enacted
- Jul 2020 Privacy Shield invalidated by the European Court of Justice (Schrems II judgement)
  - Judgment on the Schrems' petition following the enactment of Privacy Shield and GDPR
  - Not only invalidated Privacy Shield, but also pointed out the inadequacies of the then SCC
- Mar 2022 New framework, TADPF agreed in principle

1. Created from publicly available information

Source: [European Commission "Trans-Atlantic Data Privacy Framework" 2022](#); [The White House "Fact sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework" 2022](#)





## 4 SCC/MCC (1/4)

### Overview

SCC/MCC is one of the measures that enables cross-border transfer of personal data. Although it does not provide third-party certification like BCR, it is highly convenient for businesses because it is based on a contract between the parties and the contract template is publicly available. In recent years, BCR has been widely adopted and formulated not only at the national level but also at the regional level, such as in ASEAN and Ibero-America.

### Justification Basis

Each country/region regulation

### Details

#### Party to a contract

Data Exporters and (Extraterritorial/External) Data Importers

- Depending on each regulations, further subdivided into data exporter/data importer roles (e.g., controller, processor, etc.)

#### Effective period/renewal

Period of time specified in the agreement b/w the parties

#### Requirements

- SCC/MCC generally consists of the main text of the contract, which lists the parties' obligations, etc., and an annex (or table) that provides detailed information on the cross-border transfer.
- \* The main items stipulated in the main text and the main information items required in the annexes are listed on the following pages.

#### Procedures

The basic procedure for signing a SCC/MCC, which varies slightly from country to country/region to region, is as follows:

1. Assessment of the current situation and collection of necessary information
2. Selection of appropriate SCC/MCC format depending on the data transfer situation
3. Impact assessment
  - Evaluation of the data transfer situation, and the regulations/practices of the destination country, and the content of protective measures
4. Execution





## 4 SCC/MCC (2/4)

### Applicable Countries/Regions

EU	<p>Standard Contractual Clauses</p> <ul style="list-style-type: none"> <li>The first edition came into effect in 1995. The latest edition came into effect in 2021.</li> <li>4 methods are published: Controller (C)-Processor (P), C-C, P-P, P-C</li> </ul>
UK	<p>IDTA (International Data Transfer Agreement)</p> <ul style="list-style-type: none"> <li>Enforced in 2022</li> <li>2 methods are published: C-C, C-P</li> </ul>
China	<p>Standard Contract Provisions for Export of Personal Information (Draft)</p> <ul style="list-style-type: none"> <li>Began to gather public comment in June 2022.</li> <li>Only one method is drafted: Processor - Foreign Recipient</li> </ul>
New Zealand	<p>Model contract clauses for sending personal information overseas</p> <ul style="list-style-type: none"> <li>Enforced in 2020</li> <li>Only one method is published: Discloser - Recipients</li> </ul>
ASEAN	<p>ASEAN Model Contractual Clauses for Cross Border Data Flows</p> <ul style="list-style-type: none"> <li>Enforced in 2022</li> <li>2 methods are published: C-C, C-P</li> </ul>
Ibero-America	<p>Red Iberoamericana Calausulas Contractuales</p> <ul style="list-style-type: none"> <li>Enforced in 2021</li> <li>2 methods are published: C-C, C-P</li> </ul>
Singapore	No proprietary format (recommend use of ASEAN MCCs)
Brazil	Regulations define SCC as a cross-border transfer tool, but details are yet to be determined (no actual operation)

Source: [European Commission "Standard Contractual Clauses \(SCC\)";](#) [ICO "Information Data Transfer Agreement";](#) [Guān yú fā bù 《 wǎng luò ān quán biāo zhǔn shí jiàn zhǐ nán – gè rén xìn xī kuà jìng chǔ lǐ huó dòng ān quán rèn zhèng guī fàn 》 de tōng zhī](#) [Personal information outbound standard contract provisions (Draft for comment)]; [Privacy Commissioner "Sending information overseas";](#) [ASEAN "ASEAN Model Contractual Clauses for Cross Border Data Flows";](#) [Red Iberoamerica "Red Iberoamericana calausulas contractuales 2021";](#) [PDPC "Guidance for use of ASEAN MCCs in Singapore"](#)





## 4 SCC/MCC (3/4): Comparison of Major Requirements

		EU	UK	China	New Zealand	ASEAN	Ibero-America	Singapore	Brazil
Major items to be defined in the main body (e.g., general provisions)	Privacy Principles	●	●	●	●	●	●	<b>Recommends use of ASEAN MCCs</b>  Revised definition of data subject/personal data and proposed additions and modifications to clarify timing of notification in the event of a data breach	<b>Details Not determined</b>
	Processing Limitation	●	●	●	●	●	●		
	Notification	●	●	●	●	●	●		
	Accuracy	●	●	●	●	●	●		
	Security Safeguards	●	●	●	●	●	●		
	Participation/ Access	●	●	●	●	●	●		
	Accountability	●	●	●	● <sup>3</sup>	●	●		
	Other Data Protection	●	●	●	●	●	●		
	Data Minimization	●	●	●	●	●	●		
	Limited Data Retention	●	●	●	●	●	●		
	Restrictions for Sensitive Data	●	1	2	●	●	●		
	Transfer to Third Party	●	●	●	●	●	●		
	Processing records and storage	●	●	●	●	●	●		
	Rights of the Data Subject	●	●	●	●	●	●		
	Right of Access	●	●	●	●	●	●		
	Automated Individual Decision-Making	●	●	●	●	●	●		
	Right of Petition	●	●	●	●	●	●		
	Right of Remedy	●	●	●	●	●	●		
	Third Party Beneficiary	●	●	●	●	●	●		
	Third Country Law Impact Assessment	●	●	●	●	●	●		
Personal Data Breach Handling	Notification	●	●	●	●	●	●		
Dispute Resolution	Implementation of Correction	●	●	●	●	●	●		
	Record and Storage	●	●	●	●	●	●		
	Cooperation in Resolution	●	●	●	●	●	●		
Request for Disclosure by Public Auth.	Acceptance of decisions	●	●	●	●	●	●		
	Acceptance of liability of Violations	●	●	●	●	●	●		
Request for Disclosure by Public Auth.	Notification	●	●	●	●	●	●		
	Opposition	●	●	●	●	●	●		
Request for Disclosure by Public Auth.	Minimum data supply	●	●	●	●	●	●		

Note: If there is more than one format, compare by Controller - Controller content

1. Part 1, Table 2 2. Only requires notification of the necessity of the transfer and the impact of the transfer on the data subject (Article 2(2))3. No mention of responsibility for performance/compliance, but specifies that there should be a person responsible for monitoring compliance with the contract (Article 1(7))

Source: European Commission "Standard Contractual Clauses (SCC)"; ICO "Information Data Transfer Agreement"; Guān yú fā bù 《 wǎng luò ān quán biāo zhǔn shí jiàn zhǐ nán — gè rén xìn xī kuà jìng chǔ lǐ huó dòng ān quán rén zhèng guī fàn 》 de tōng zhī [Personal information outbound standard contract provisions (Draft for comment)]; Privacy Commissioner "Sending information overseas"; ASEAN "ASEAN Model Contractual Clauses for Cross Border Data Flows"; Red Iberoamerica "Red Iberoamericana calausulas contractuales 2021"; PDPC "Guidance for use of ASEAN MCCs in Singapore"





## 4 SCC/MCC (4/4): Comparison of Other Requirements

● : Applicable    ● : Option

		EU	UK	China	New Zealand	ASEAN	Ibero-America	Singapore	Brazil
Items that need to be described in annexes, etc.	Party Information	Company Name	●	●	●	●	●	<b>Recommends use of ASEAN MCCs</b> Revised definition of data subject /personal data and proposed additions and modifications to clarify timing of notification in the event of a data breach.	<b>Details Not determined</b>
		Role (Controller, etc.)	●	●	●		●		
		Contact Information	●	●	●				
	Data Subject	Type	●	●	●	●	●		
	Personal Data	Data Type (Name, etc.)	●	●	●		●		
		Data Volume			●				
		Information about Tech. and Org. Measures	●	●	●		●		
		Restrictions for Sensitive Data/Additional Safeguards	●		● <sup>2</sup>		●		
	Details of Transfer/Processing	Objectives	●	●	●	●	●		
		Transfer Frequency	●		●		●		
		Character of Processing	●						
		Processing/Storage Period	●	●	●		●		
		Third-Party Transfers		●	●		●		
	Relationship to Relevant Regulations/Documents	Governing Law	<sup>1</sup>	●	●		●		
		Impact of Regulations/Contracts in the Transferring Country	<sup>1</sup>	●					
	Relevant Authority (Data Protection Agency, etc.)			● <sup>3</sup>			●		

Note: If there is more than one format, compare by Controller - Controller content

1. Provided for in the main body (Article 4, 5 and 17) 2. Need to explain only types of sensitive data (Annex 1) 3. Description of the arbitral tribunal

Source: European Commission "Standard Contractual Clauses (SCC)"; ICO "Information Data Transfer Agreement"; Guān yú fā bù 《 wǎng luò ān quán biāo zhǔn shí jiàn zhǐ nán – gè rén xìn xī kuà jìng chǔ lǐ huó dòng ān quán rèn zhèng guī fàn 》 de tōng zhī [Personal information outbound standard contract provisions (Draft for comment)]; Privacy Commissioner "Sending information overseas"; ASEAN "ASEAN Model Contractual Clauses for Cross Border Data Flows"; Red Iberoamerica "Red Iberoamericana calausulas contractuales 2021"; PDPC "Guidance for use of ASEAN MCCs in Singapore"





## 6 BCR (1/3)

### Overview

BCR is a certification scheme that approves cross-border transfers of personal data within a group of businesses. In addition to the EU, the UK and other countries with GDPR-like cross-border transfers are increasingly adopting similar mechanisms as a basis for cross-border transfers (Brazil, Singapore, etc.).

BCR may appear to be more useful for cross-border transfers within a group of businesses, since only one application is covered under the BCR, even in situations where the SCC/MCC requires the transfer to be divided into multiple contracts. However, BCR does not have a specific contract template published like the SCC/MCC, and businesses need to document each contract individually, which in practice entails significant costs. For this reason, only few companies use BCR.

Since the provisions of GDPR are the most detailed, we will describe BCR in GDPR.

### Justification Basis

Each Country/Region Regulation

### Details

#### Application/Certification Subject

Entities that plan to transfer personal data across borders within a group of businesses or a group of businesses engaged in joint economic activities

#### Authorization Agency

Competent Data Protection Authority

#### Number of Certified Businesses

38 approved businesses since GDPR went into effect (as of September 2022) <sup>1</sup>

#### Requirements

<Approval Requirements (Article 47(1))>

- BCR is legally binding, applies to all relevant members, and is complied with
- BCR clearly states the enforceable rights of data subjects with respect to the processing of their personal data
- BCR meets the requirements set out in Article 47(2) of GDPR (required entries to the next page)

1. As of September 2022 (EDPB "Approved Binding Corporate Rules")

Source: JETRO "EU Ippan deta hogo kisoku ni kakawaru jitsumu hanndobukku [EU GDPR Operation Handbook]," 2017; JAPDEC "Ippann deta hogo kisoku (GDPR) kari nihongo yaku [GDPE (Japanese)]," 2016





## 6 BCR (2/3)

### <Required Items (Article 47(2))>

- a. The details of target operator
- b. The type of processing, its purposes, data subjects affected
- c. Their legally binding nature, both internally and externally
- d. The application of the general data protection principles
- e. The rights of data subjects in regard to processing and the means to exercise those rights
- f. Confirmation that operators in the EU assume responsibility for BCR violations by non-EU operators
- g. How the information on the BCR to the data subjects
- h. The tasks of the data protection officer
- i. The complaint procedures
- j. The mechanisms to ensure the verification of compliance with the BCR (shall include methods for ensuring corrective actions)
- k. The mechanisms for reporting and recording changes to the rules
- l. The cooperation mechanism with the supervisory authority to ensure compliance
- m. The mechanisms for reporting to the competent supervisory authority any legal requirements to which are likely to have a substantial adverse effect on the guarantees provided by the BCR
- n. The appropriate data protection training to personnel having permanent or regular access to personal data

### Procedures

1. Collection of necessary information and compliance with requirements (e.g., data mapping)
2. BCR application by the operator to the competent data protection authority
3. Examination and preparation of draft decision including relevant data protection authorities, notification to the European Data Protection Board
4. Opinion and final decision by the European Data Protection Board
5. Approval of BCR by the competent data protection authority

### Time required for Certification (approximately)

Several Years<sup>1</sup>

### Renewal and Cancellation

- Approval is valid until amended, replaced or withdrawn by the competent Data Protection Authority as required
- Any updates must be submitted to the Data Protection Authority, but may be reviewed annually, unless the changes affect the level of personal data protection or have other significant consequences.

1. From expert interview

Source: JETRO "EU Ippan deta hogo kisoku ni kakawaru jitsumu hanndobukku [EU GDPR Operation Handbook]," 2017; JAPDEC "Ippann deta hogo kisoku (GDPR) kari nihongo yaku [GDPE (Japanese)]," 2016





## 6 BCR (3/3) : Comparison on Requirements

● : Applicable ● : Option

	EU	UK	Singapore	Brazil
Justification Basis	GDPR Article 47	UK GDPR Article 47	PDPR Article 11	
Approving Authority/Application to	Competent Supervisory Authority	ICO	—	
Application/Certification Subject	Business groups or a business within the group engaged in joint economic activity	Business groups engaged in joint economic activities and all related parties within the group	The transferrer and Organizations related to the transferrer	
Number of Certified Businesses	38 companies <sup>1</sup>	27 companies <sup>2</sup>	N/A	
Basic Requirements	<ul style="list-style-type: none"> <li>Legally binding and adhered to by all members</li> <li>Clear statement of enforceable rights of the data subject</li> <li>Statement of Required Information</li> </ul>		<ul style="list-style-type: none"> <li>The transferee has a relationship with the transferrer and is not subject to any other legally binding obligation</li> </ul>	
Required Information	Information on the Parties involved	●	●	Details Not determined
	Internally/Externally Binding	●	●	
	Information on Transfers	● <sup>3</sup>	● <sup>3</sup>	
	Application of General Data Protection Principles	●	●	
	Data Minimization	●	●	
	Limitation of Retention Periods	●	●	
	Legal Basis for Data Handling	●	●	
	Sensitive Data Handling	●	●	
	Re-transfer to third parties	●	●	
	Right not to be subject to decisions based solely on automated processes	●	●	
	Right to file an objection/seek relief/compensation	●	●	
	Acceptance of Liability	●	●	
	Methods of providing information to data subject	●	●	
	Establishment of Data Protection Officer	●	●	
	Complaint filing/processing procedures	●	●	
	Mechanisms to ensure BCR compliance	●	●	
	Reporting and Recording of BCR change	●	●	
	Cooperation with Supervisory Authorities	●	●	
	Data Protection Training	●	●	
Other	Identification and reporting of third country laws with adverse effects	Identification and reporting of third country laws with adverse effects	Not Specified Only required to state "rights and obligations provided for in the BCR"	

1. as of September 2022 (EDPB "Approved Binding Corporate Rules") 2. no distinction made b/w Controller and Processor; 22 approved under DPA2018, 5 approved under UK GDPR. as of September 2022 (ICO "List of BCR Holders") 3. GDPR/UK GDPR requires data subject/personal data type, purpose of transfer, type of treatment, and details of transfer to third country, while PDPR requires only the scope of transfer (country) to be stated Source: UK GDPR; GDPR; Personal Data Protection Regulations 2021





## 7 Outbound Data Transfer Security Assessment (1/2)

### Overview

Outbound data transfer security assessment is to assess the security of personal and Important data collected/generated through operations in China

### Background

Safety assessment was developed in the three data laws, and detailed procedures were defined in “Measures for outbound data transfer security assessment” in September 2022

### Justification Basis

China's three data laws and “Measures for outbound data transfer security assessment”

### Details

#### Application/Certification Subject

Businesses that fall under any of the following (Measures for outbound data transfer security assessment Article 4)

- ① Businesses planning to provide Important data outside of China
- ② Major IT infrastructure operators or data handlers who handle personal data of more than 1 million individuals
- ③ Businesses that have provided personal data of 100,000 individuals or sensitive personal data of 10,000 individuals outside the region since Jan 1 of the previous year and who plan to transfer personal data outside China
- ④ Other businesses falling under the requirements set by the cyberspace administration of China (CAC)

#### Authorization Agency

Cyberspace Administration of China

- Strictly speaking, applications are filed through the local CAC

#### Number of Certified Businesses

N/A

#### Requirements

Outbound data transfer security assessment includes the following items

<Self-assessment of cross-border data transfer risk (Article 5)>

- ① Legality, legitimacy, and necessity of the purpose of cross-border data transfer and processing of personal data by the overseas recipient
- ② Scale, type, degree of sensitivity of cross-border data, and possible risks to national security
- ③ Responsibilities of overseas recipients, and administrative and technical measures to fulfill those responsibilities
- ④ Risks of tampering during and after data transfer, and methods of protecting the rights and interests of personal data
- ⑤ Adequacy of cross-border data transfer contracts or responsibilities and obligations for data security protection arrangements in other legal documents with overseas recipients
- ⑥ Other potential issues that may affect security of cross-border data

Source: JETRO “Deta ikigai itenn annzenn hyouka bennpou 9gatsu1nichi kara shikou [Measures for outbound data transfer security assessment, enacted on 1 Sep, to clarify the scope of safety assessment].” 2022.; shù jù chū jìng ān quán píng gū bàn fǎ [Outbound Data Transfer Security Assessment]





## 7 Outbound Data Transfer Security Assessment (2/2)

### Procedures

The procedures set by the Measures for outbound data transfer safety assessment are as follows

1. Self-assessment of cross-border data transfer risk
2. Application to local CAC
3. Integrity assessment by the provincial CAC (check incomplete documents, etc., within 5 working days)
4. Provincial CAC sending applications to the state CAC
5. Decision of acceptance by the state CAC (within 7 working days)
6. Security evaluation by the state CAC and related agencies (within 45 working days)
7. Notification of evaluation results to the applicant

### Time required for Certification (approximately)

approximately 2 months after submitting documents to CAC

### Renewal and Cancellation

- 2 years after the evaluation results
  - If changes occur during the validity period, or cross-border transfer continues after the validity period, re-assessment is required (Article 14)
  - CAC determines correction or termination of cross-border data transfer when it finds the assessed cross-border data transfers no longer meet the requirements (Article 17)





# 8 Certification of Personal Information Cross-Border Processing Activities

## Overview

This certification is a mechanism to certify that domestic/foreign businesses comply with requirements for cross-border transfers of personal data. It is defined as one of the requirements for cross-border transfer in PIPL. It is not regarded as a requirement for cross-border transfers as of Sep 2022, since some requirements for the certification including certification bodies are undecided, although Guidelines were published in 2022

## Justification Basis

- China PIPL (Article 38.1)
- Guidelines (Guidance on Network Security Standardized Practice: Technical Specification for Certification of Personal Information Cross-Border Processing Activities)

## Details

### Application/Certification Subject

- Multinational businesses engaging in cross-border processing of personal data between subsidiaries or affiliates<sup>1</sup>
- Personal data operators outside of China to which PIPL Article 3.2 applies

Application/certification unit  
Corporation

Authorization Agency  
TBD

Number of Certified Businesses  
N/A

1. Application for certification must be made by the party in China. In the case of PIPL Article 3.2, the application must be made by a specialized body or a designated representative (Guideline, Article 2) 2. Guó jiā biāo zhǔn 《 gè rén xìn xī ān quán guī fàn 》2020 bǎn zhèng shì fā bù [National standard "personal information security specification" 2020 version] Source: National Information Security Standardization Technical Committee "Guān yú fā bù 《 wǎng luò ān quán biāo zhǔn shí jiàn zhǐ nán-gè rén xìn xī kuà jìng chǔ lǐ huó dòng ān quán rèn zhèng guī fàn 》 de tōng zhī [Notice on the release of the "Cybersecurity Standards Practice Guide-Security Certification Specifications for Cross-Border Processing Activities of Personal Information]," 2022, Corporate Legal Navigation "Kojin jouhou ekkyou shori hogo ninshou kihann no kaisetsu [Explanation of personal information cross-border processing certification]", 2022

## Requirements

- Parties applying for certification must comply with the Personal Data Security Code<sup>2</sup> as a precondition
- In addition, the following basic principles and requirements set in the Guidelines should also be observed for cross-border transfers

### <Basic principles>

- ① Principles of legality, legitimacy, necessity, and integrity
- ② Principles of openness and transparency
- ③ Principle of quality information
- ④ Principle of equal protection
- ⑤ Principle of accountability
- ⑥ Principle of self-accreditation

### <Basic requirements>

- ① Legally binding contracts
- ② Organizational control system (appoint chief privacy officer and build a privacy protection org)
- ③ Compliance with the uniform rules for cross-border processing of personal data
- ④ Preliminary personal data protection impact assessment

Procedures/Time required for Certification (approximately)  
TBD

Renewal and Cancellation  
TBD





## 9 CBPR (1/2)

### Overview

The CBPR is one of the international systems that assesses and certifies compliance with the APEC Privacy Framework for the cross-border transfer of personal data by businesses. Nine APEC member economies including JP and the US participate in the CBPR (as of Apr 2022).

In Japan and Singapore, the Personal Information Protection Law/Guidelines use CBPR as one of the tools to realize cross-border transfer, recognizing it as an “appropriate measure to ensure adequate level of protection”

### Background

Based on the APEC Privacy Framework approved in 2004, it was developed in 2011 following the 2009 CPEA (Cross-border Privacy Enforcement Arrangement) through the “APEC Data Privacy Pathfinder Project” launched in 2008

### Justification Basis

APEC Privacy Framework

### Details

#### Application/Certification Subject

Businesses (in Japan, the business must be an “Accredited Personal Information Protection Organization” certified by JIPDEC)

#### Authorization Agency

Accountability agents, third-party certification bodies, conduct examinations and accreditation

- Accountability agents are independent organizations accredited by APEC
- 9 bodies in 5 of the 9 countries participating in CBPR have been accredited<sup>1</sup>
- In Japan, JIPDEC is certified as an accountability agent

#### No. of certificated companies

52 companies (as of Sep 2022)<sup>2</sup>

- US: 42 companies, Japan: 4 companies, Singapore: 6 companies

#### Requirements

Certification standards published by JIPDEC and requirements for application are shown on the next page

#### Procedures

1. Collection/handling of required information and preliminary confirmation
2. Application for CBPR certification by an organization
3. Assessment (document assessment/on-site assessment)
4. Certification decision
5. Announcement of certified organization by accountability agent and notification to APEC Secretariat

#### Time required for Certification (approximately)

4 months

#### Renewal and Cancellation<sup>3</sup>

- APEC does not allow renewal audits and requires annual recertification applications
  - Some companies do not apply for recertification every year
- Monitoring is done to check the system and handled data, and if any problems are found, guidance, suspension of certification, or cancellation of certification will be given depending on the nature of the problem

1. As of September 2022 2. [CBPRs "Compliance Directory"](#) 3. [JIPDEC "CBPR ninshou no igi to kinji no shutoku doukou ni tsuite \[Significance of CBPR Certification and recent application trends\]" 2022](#)

Source: [JIPDEC "APEC CBPR ninshou sinnsei gaidobukku 2.3 \[APEC CBPR certification application guidebook ver.2.3\]" 2022](#)





## 9 CBPR (2/2)

### CBPR Certification Standards

JIPDEC has published the following JIPDEC criteria based on the CBPR Guidelines to confirm compliance with the APEC Privacy Framework

- 1.1 Compliance with APEC Information Privacy Principles
- 1.2 Identification of personal information
- 1.3 Identification of the purpose of use
- 1.4 Laws, guidelines, and other codes stipulated by the state
- 1.5 Recognition, analysis of risk
- 1.6 Internal regulations
- 1.7 Emergency responses
- 2.1 Privacy policy
- 3.1 Appropriate acquisition of personal information
- 4.1 Measures concerning use
- 4.2/8.5 Measures concerning provision of personal information
- 5.1/7.7 Option for the individual, and discontinuance of use or provision of personal information
- 5.2 Securement of accuracy of personal information
- 6.1/6.3 Risk treatment, and the establishment of security control measures
- 6.2 Identifying, analyzing and evaluating personal information protection risks
- 6.4/8.6 Supervision of trustees
- 6.5 Periodic review
- 7.1 Public disclosure of the matters concerning personal information
- 7.2/7.3/7.5/7.6 Rights of the individual concerning personal information
- 7.4 Notification regarding purpose of use of personal information
- 8.1 Resources for establishing and maintaining its personal information protection management system
- 8.2 Responses to complaints and consultation
- 8.3/8.4 Supervision and training of employees
- 9.1/9.2 Regular internal audit
- 9.3 Corrective actions and preventive actions

### Information required when applying for CBPR certification

1. CBPR application form
2. CBPR system preliminary questionnaire  
Major items in the preliminary questionnaire include
  - Basic information
    - Addresses, roles, and other details of the organization applying for certification and subsidiaries/branches controlled by the organization
    - Information on the responsible person
    - Details of the business/operations handling personal data
    - Countries/regions where personal data will be acquired or transferred
  - Notification: Status of reflecting requirements in the privacy statement
  - Acquisition
    - Personal data acquisition requirements
    - Personal data acquisition methods
  - Usage: Personal data use requirements
  - Options: Status of presenting options on acquisition, use, and disclosure of personal data
  - Integrity of personal data: Accuracy, completeness, and update of personal data acquired
  - Security measures: Status of implementation of security measures
  - Access and correction: Responses to access and correction of personal data
  - Responsibility: Systems and measures to fulfill responsibilities for compliance with CBPR requirements
3. JIPDEC additional questionnaire
  - Detailed information on transfer confirmed in the preliminary questionnaire: Legal basis for transfer, estimated data volume, etc.
  - Responses and basis information for JIPDEC criteria
4. Incident list for the past 6 months





## 10 PRP Certification (1/2)

### Overview

PRP certification is a system that certifies on behalf of data controllers that data processors have a level of protection for personal data that conforms to the APEC Privacy Framework when processing. Because of its limited scope, it focuses on two of the APEC Privacy Framework principles (safeguards and accountability) and has fewer requirements than the CBPR.

Singapore recognizes PRP certification as one of the requirements under the PDPA/PDPR for "adequate measures to ensure an adequate level of protection" to permit cross-border transfer.

### Background

It was developed in 2015 as an ancillary certification to CBPR specifically for data processors who process personal data on behalf of data controllers. Compared to CBPR, only the US and Singapore are participating as of 2020.

### Justification Basis

APEC Privacy Framework

### Details

#### Application/Certification Subject

Businesses (Processor)

#### Authorization Agency

Assessment Body (AB)

### Number of Certified Businesses

44 companies (as of September 2022)

- US: 41 companies, Singapore: 3 companies

### Requirements

APEC defines the following requirements (presented by AB as Self-Assessment Sheet)

#### 1. Application Information

- Basic Information
  - Addresses, roles, etc. of the organization applying for certification and any subsidiaries/branches controlled by the organization
  - Contact person information

#### 2. Questions

- Implementation status and details of the information security policy
- Status of employee training
- Status of implementation of safeguards (effectiveness testing, notification process to managers, etc.)
- Procedures for disposal and return of personal data
- Status of use of risk assessment
- Implementation of limitation of purposes of use of personal data
- Details of the process for responding to management instructions
- Establishment of responsible person
- Status of response to notification to the controller





## 10 PRP Certification (2/2)

### Procedures

1. Gathering and handling of information, prior confirmation (Self-Assessment)
2. Application for PRP certification by the operator
3. Audit by AB (Both document and on-site)
4. Decision on certification
5. Publication of certified business by AB

### Time required for Certification (approximately)

N/A

### Renewal and Cancellation

- Basic requirements are the same as CBPR
  - The certification period is one year, and recertification application is required every year.
  - The AB must be notified of any significant changes to the contents of the application. Depending on the content, an audit may be required, and the AB will determine the validity of the certification.





# 11 Codes of Conduct (1 / 2)

## Overview

Codes of Conduct are rules established by industry associations for various industries of various regulations, not only for cross-border transfers, and are created for the purpose of concretizing the applicable regulations. Cross-border transfer-related regulations, including the GDPR, are recognized as one of the tools for cross-border transfers in several countries, and as of September 2022, there are three countries/regions that provide codes of conduct as a basis for cross-border transfers: Europe, the UK, and Brazil. Since both the UK and Brazil base their regulations on GDPR, this section details the Codes of Conduct in GDPR.

## Codes of Conduct in EU GDPR

### Justification Basis

GDPR Article 40

### Adoption to Cross-Border Transfers

- Cross-border data transfers outside the EU are permitted if the transferee company complies with the Codes of Conduct and has adequate safeguards in place that are binding and enforceable, including data subject rights (Article 40(3))
- For the Codes of Conduct to be applicable to operators in third countries, it must be submitted to the European Data Protection Council (Article 40(7))

### Application/Certification Subject

Associations and other bodies representing categories of controllers or processors (Article 40(2))

### Authorization Agency

Competent Supervisory Authorities

## Requirements

Article 40(2) provides details of what should be included (see next page).

## Procedures

CoC establish two procedures: one for the intended handling of data in one country and one for the intended handling of data in multiple countries. This section details the procedures to be followed when data is to be handled in multiple countries from the perspective of cross-border transfers. (Article 40(7)-(11))

1. Submit draft of Codes of Conduct or proposed amendments or extensions to existing Codes of Conduct to the supervisory authority
2. Submit documents from the supervisory authority to the European Data Protection Board
3. Review and opinion by the European Data Protection Council
4. Approval of the Codes of Conduct by the Supervisory Body following the opinion of the European Data Protection Council
5. Submit opinion from the European Data Protection Board to the European Commission
6. Decision by the European Commission on the validity of the Codes of Conduct (adoption of implementing legislation)
7. Publication of the approved Codes of Conduct by the European Commission
8. Registration and start of use of the approved Codes of Conduct by the European Data Protection Board

## Renewal and Cancellation

- Although no specific period of validity is set, the approved Codes of Conduct is subject to monitoring for compliance. If a business is found not to be in compliance with the Codes of Conduct, appropriate action will be taken (Article 41(4)).
  - Monitoring is carried out by a specific accreditation body accredited by the supervisory authority (Article 41(1))





## 11 Codes of Conduct (2/2)

- Of the three countries/regions that have adopted Codes of Conduct, Brazil has not yet implemented them as of September 2022, as detailed implementation rules have yet to be determined.
- CoC in operation in EU/UK are designed based on the UK GDPR, so there is no difference in requirements.
- Like the BCR, CoC only list requirements in the regulation and are not as specific as the SCC. Thus, each organization must embody and document each requirement based on industry practices and characteristics.
- However, the GDPR allows for the creation of CoC across multiple countries (including outside the EU), which has the advantage of creating the same level of protection and facilitating the cross-border transfer of personal data both inside and outside the EU
  - For example, BigTech (Meta, Google, etc.) in the US, which has been ruled in violation of the GDPR, has also agreed to an EU CoC regarding false information.

● : Applicable  
● : Option

	EU	UK	Brazil
Justification Basis	GDPR Article 40	UK GDPR Article 40	
Approving Authority/Where to apply	Competent Supervisory Authority	ICO	
Applicant/Parties	Associations and other org. representing various types of Controller or Processors	Associations and other org. representing the Controller or Processor category	
Items to be included in the Codes of Conduct	Treatment with fairness and transparency	●	Details not Determined
	Legitimate interests required by the controller in specific circumstances	●	
	Collection of personal data	●	
	Pseudonymization of personal data	●	
	Information provided to the public/data subjects	●	
	Exercise of Data Subject's Rights	●	
	Information provided to children and obtaining parental consent	●	
	Responsibility of the controller and data protection measures in the initial setup, etc., as well as measures to ensure the security of data processing	●	
	Notification of a breach to the supervisory authority/data subject	●	
	Transfer to third countries/international organizations	●	
	Dispute resolution procedures b/w the controller and the data subject	●	











## 2.4

# Details of the Results: Other Relevant Tools



## Other Relevant Tools

The main data protection-related tools used in the countries/regions surveyed

		Title	Country/Region	Applicable laws/Standards	Application/Certification subject
Personal Data Protection 	Certification 	1 GDPR-CARPA	EU (Luxenberg)	GDPR, ISO Standards, etc.	Businesses, Public Organization Other Organizations, etc.
		2 dp.mark	Taiwan	PDPA (Taiwan), Other International Rules, etc.	Businesses
		3 Data Protection Trust Mark (DPTM)	Singapore	PDPA/PDPR (Singapore)	Non-Public Organizations
		4 ISMS-P Certification	South Korea	PIPA (South Korea)	Data Communication Service Providers, etc.
		5 Privacy Mark (P Mark)	Japan	P Mark Operation Guidelines (Compliant JIS Q)	Businesses
		6 JAPHIC Mark	Japan	APPI (Japan), Other Relevant Guidelines	Businesses
		7 EuroPriSe	Germany	EuroPriSe Standards ※Compliant GDPR	IT Product, IT-related Service Vendors
		8 TRUSTe Mark	Global	OECD Privacy Guidelines	Domain, Application
		9 CNIL Certification (Certification des compétences du DPO)	France	EU GDPR, France Data Protection Regulations	Processor of Personal Data
		10 ISMS-PIMS Certification <sup>1</sup>	Global	ISO/IEC 27701	Businesses, Divisions within a business
	Standard 	11 Personal Information Security Specification	China	—	—
		12 JIS Q 15001	Japan	—	—
General Data Protection 	Certification 	1 ISMS Certification <sup>1</sup>	Global	ISO/IEC 27001	Businesses, Divisions within a business
		2 WebTrust	Global	WebTrust Standard	Businesses (Electronic authentication service providers)
	Standard 	3 NIST SP800 Series	US	—	—
		4 SOC2 (Service Organization Control Type2)	US	—	—

1. Some of the ISO/IEC standards have a conformity assessment system. ISO/IEC 27001 and 27701 are classified here as certifications rather than standards because they both have conformity assessment systems.



## Summary (1/4)

Personal data protection tools exist based on national/regional regulations. Certain commonalities can be seen, and some tools are being linked and connected.



In the field of personal data protection, **there are many certifications based on domestic regulations**. In the field of general data protection (incl. security), on the other hand, international certification is widespread. And in recent years, from a security perspective, **the US has established evaluation standards for data protection (security) standards**, which are becoming more widespread globally.

- Many countries, especially in Asia, have personal data protection certification based on each domestic regulation.
- EU also has a certification based on GDPR, but only GDPR-CARPA has been approved by the EU.
- In North America, which does not have a comprehensive law, there is a certification (TRUSTe Mark) that aims to "ensure trust for sound business use of personal data."



**The requirements of the various certifications are generally the same for major items.**

- For detailed items, **Asian countries tend to have more requirements for organizational safeguards**, while **EU countries tend to define technical requirements** in more detail.



**Personal data protection certification is also being connected** with cross-border transfer tools.

- **Taiwan recommends** that personal data protection certification (Dp.mark) and cross-border transfer certification (CBPR) be combined to promote efficient data protection and transfer.
- The EU stipulates that certification approved in accordance with a specific process can be used as a basis for cross-border transfers (GDPR Article 46), and GDPR-CARPA fulfills this requirement, **but currently only within the EU (Luxembourg)**.<sup>1</sup>
- China is also developing a system in which compliance with personal data protection standards is a prerequisite for certification of cross-border transfers, **but since it only measures the level of personal data protection of the domestic businesses and doesn't cover both parties** involved in the cross-border transfer, other tools like SCC/MCC, etc. is necessary. (Strictly speaking, the cross-border transfer tool and the personal data protection tool are not connected.)

1. When data is transferred from the EU (Luxembourg), it certifies the GDPR compliance of the EU (Luxembourg) operator at the source of the transfer and does not certify the destination outside the EU (e.g., Japan). Therefore, it does not function as a mutual certification for cross-border transfers.



## Summary (2/4): Comparison between Personal Data Protection Tools

There are differences because of its purpose of each tool, as well as in the coverage of the basic privacy principles

			1 GDPR -CARPA	2 dp.mark	3 DPTM	4 ISMS-P	5 Privacy Mark	6 JAPHIC Mark <sup>1</sup>	7 EuroPriSe	8 TRUSTe Mark	9 CNIL	11 China Sec. Specification
			✓	✓	✓	✓	✓					✓
Connection with other tools			Based on GDPR Article46	Recommend to be obtained with CBPR	Connection with ISMS	Connection with ISMS	Based on JISQ				Defined only as relevant to the responsible person	Mandatory for data transfer
Basics	Privacy Principles	Processing Limitation	●	●	●	●	●	●	●	●		●
		Notification	●	●	●	●	●	●	●	●		●
		Accuracy	●	●	●	●	●	●	●	●		
		Security Safeguards	●	●	●	●	●	●	●	●		●
		Participation/Access	●	●	●	●	●	●	●	●		●
		Harm Prevention						●				
		Accountability	●	● <sup>2</sup>	●		● <sup>2</sup>		●	● <sup>2</sup>		●
	Restrictions for Sensitive Data		●	●	●	●	●	●	●	●		●
	Risk Assessment		●	●	●	●	●		●	●		●
	Record of Processing Activities		●	●	●	●	●	●	●	● <sup>5</sup>		●
Transfer/Outsource	Tech and Org Safeguards		●	●	●	●	●	●	●	●		●
	Assessment	Documentation	●	●	●	●	●	●	● <sup>4</sup>	●	※See following pages	●
		Supervision	●	●		●	●	●	● <sup>4</sup>	●		●
		Safeguards of Transfer	●	●	●	●	●	●	●	●		●
			●	●	●	●	●	●	●	●		●
Transfer/Outsourcing	Right of Access		●	●	●	●	●	●	●	●		●
	Automated Individual Decision-Making		●	●					●			●
	Right to Object		●	●	●	● <sup>3</sup>	●	●	●	●		●
	Right of Data Portability		●	●	●		●	●	●	●		●
	Children's Rights		●	●					●	●		●

Note: Privacy Mark includes JIS Q15001, thus JIS Q 15001 is excluded from this comparison. ISMS-PIMS is also excluded because specific requirements are undisclosed.

Source: HPs of various governing bodies, etc.

1. Use [Kojouhou Tsuusokuhen \[PIPL General Rules\]](#) 2. Require commitment for the performance from the management level. 3. The measures required to guarantee the rights of data subjects are access to personal data, correction and deletion, suspension of processing, objection, and response to requests for withdrawal of consent, with no mention of disclosure or reproduction of personal data. 4. Separate definitions for processors, joint controllers, etc. 5. Require records only with respect to third-party provisioning activities.



# Summary (3/4) : Comparison of Technical Safeguards Requirements

Comparison based on items presented in EU SCC; technical measures tend to be defined in more detail in the EU tool

	1 GDPR -CARPA	2 dp.mark	3 DPTM	4 ISMS-P	5 Privacy Mark	6 JAPHIC Mark <sup>1</sup>	7 EuroPriSe	8 TRUSTe Mark	9 CNIL	11 China Sec. Specification
● : Applicable										
Pseudonymization and encryption	●		2	●	Only implementation of appropriate protective measures required <sup>5</sup>	●	●	●	Defined only as relevant to the responsible person	●
Ensuring confidentiality, integrity, availability	●	●		●			●	●		
Ensuring data availability and restoration of access in event of incident	●			●			●	●		
Regular testing to ensure security of processing	●	●	●	●			●	●		
User identification and authorization	●	●		●		●	●	●		
Protection of data during transfer	●			●			●	●		
Protection of data during storage	●			●		●	●	●		
Ensuring physical security of locations where personal data is processed	●	●	3	●		●	●	●		
Ensuring event logging	●			●		●	●	●		
Ensuring system configuration	●	●	4	●		●	●	●		
Internal IT and IT security governance and management	●	●		●		●	●	●		●
Assurance/certification of processes/products	●	●	4	●			●	●		
Data minimization	●	●		●		●	●	●		
Data quality	●	●	●	●		●	●	●		
Limited data retention	●		●	●		●	●	●		●
Accountability	●						●			
Data portability	●						●	●		

Note: Compare based on EU SCC Annex II, Source: Website of various authorities, etc. JIS Q 15001 and ISMS-PIMS certifications are excluded from this comparison (see previous page)  
Source: HPs of various governing bodies, etc.

1. Use [Kojouhou Tsuusokuken \[PIPL General Rules\]](#) 2. There is no requirement for anonymization itself, although there is a requirement to document the policy regarding anonymization at the time of storage. ([DPTM Checklist Principle3 #5](#)) 3. Just required "administrative, technical and physical safeguards", but no specifics ([DPTM Checklist Principle3 #1](#))  
4. No specific measures are described, but data protection design during system development is required. ([DPTM Checklist Principle1 #7](#)) 5. [Privacy Mark Guideline J.9.2](#)



## Summary (4/4): Comparison of Organization Safeguards Requirements

While there are no major differences in the requirements for organizational safeguards overall, there are significant differences in the specificity of the content, particularly in Asia, where they are specified in more detail.

			1	2	3	4	5	6	7	8	9	11
			GDPR-CARPA	dp. mark	DPTM	ISMS-P Cert.	Privacy Mark	JAPHIC Mark1	Euro PriSe	TRUSTe Mark	CNIL Cert.	China Sec. Specification
Basics	Assessment		●	●	●	●		●		●	Defined only as relevant to the responsible person	●
	Establish responsible person		●	●	●	●	●	●	●	●		●
	Establish data protection policy		●	●	●	●	●	●	●	●		●
	Education & training		●	●	●	●	●	●		●		●
	Assessment (internal audit) /Improvement		●	●		●	●	●		●		●
Details	Risk Response	Notification to data subjects			●		●		●	●		●
		Notification to competent authorities		●	●				●	●		●
		Documentation of events/responses					●		●			●
	Claim Handling	Establishment of a contact point	●	●	●	●	●	●		●		●
		Disclosure of reasons for refusal	●	●		●	●	●				●
Note		Require documentation of decisions affecting data protection and details of safeguards				Require documentation of various matters, including data flow and other system-related documentation		Require documentation of various rules and regulations. More than 10 rules are required to be documented, ranging from emergency response to penalties.				

Note: Comparison of JIS Q 15001 alone is omitted because Privacy Mark includes JIS Q 15001; ISMS-PIMS certification is excluded from detailed comparison because specific requirements are undisclosed; 1. Use [Kojouhou Tsusokuhen \[PIPL General Rules\]](#)  
Source: HPs of various governing bodies, etc.





## Other Relevant Tools

The main data protection-related tools used in the countries/regions surveyed

	Title	Country/Region	Applicable laws/Standards	Application/Certification subject
Personal Data Protection 	Certification 	1 GDPR-CARPA	EU (Luxenberg)	GDPR, ISO Standards, etc.
		2 dp.mark	Taiwan	PDPA (Taiwan), Other International Rules, etc.
		3 Data Protection Trust Mark (DPTM)	Singapore	PDPA/PDPR (Singapore)
		4 ISMS-P Certification	South Korea	PIPA (South Korea)
		5 Privacy Mark (P Mark)	Japan	P Mark Operation Guidelines (Compliant JIS Q)
		6 JAPHIC Mark	Japan	APPI (Japan), Other Relevant Guidelines
		7 EuroPriSe	Germany	EuroPriSe Standards ※Compliant GDPR
		8 TRUSTe Mark	Global	OECD Privacy Guidelines
		9 CNIL Certification (Certification des compétences du DPO)	France	EU GDPR, France Data Protection Regulations
		10 ISMS-PIMS Certification <sup>1</sup>	Global	ISO/IEC 27701
	Standard 	11 Personal Information Security Specification	China	—
		12 JIS Q 15001	Japan	—
General Data Protection 	Certification 	1 ISMS Certification <sup>1</sup>	Global	ISO/IEC 27001
		2 WebTrust	Global	WebTrust Standard
	Standard 	3 NIST SP800 Series	US	—
		4 SOC2 (Service Organization Control Type2)	US	—

1. Some of the ISO/IEC standards have a conformity assessment system. ISO/IEC 27001 and 27701 are classified here as certifications rather than standards because they both have conformity assessment systems.





# 1 GDPR-CARPA

## Overview

GDPR-CARPA is an external certification system that certifies compliance with GDPR by Luxembourg businesses and others. Certification promotes transparency and GDPR compliance and allows data subjects to easily determine the level of information protection of their products and services.

## Background

It was adopted in May 2022 as one of the certifications and seals recommended by the EU under Article 42 of the GDPR. The CNPD (Commission Nationale pour la Protection des Données) drafted it in 2018, and after nearly four years of correspondence, it has been adopted by the EDPB (European Data Protection Board). The GDPR encourages the adoption of certification and seals, but as of now (September 2022), GDPR-CARPA is the only certification mechanism recognized under the GDPR.

## Justification Basis

- GDPR (Article 42, Article 55-56, etc.)
- ISAE 3000
- ISCQ 1
- ISO 17065

## Details

### Application/Certification Subject

Businesses, public authorities, associations and other organizations established in Luxembourg

### Application/Certification Unit

Legal Person/Corporation

### Authorization Agency

- Operation : CNPD
- Auditing : Certification bodies approved by CNPD

### Number of Certified Businesses

N/A

### Requirements

The certification criteria consist of three sections

- Section1 : Accountability Criteria / Governance Criteria
  - Applies to controllers and processors
  - Policies and procedures, records of processing activities, data subject rights, DPO, data breaches, etc.
- Section2 : Principles relating to processing of personal data (Controller)
  - Applies to controllers
  - Compliance with key data protection principles under Article 5 of the GDPR
- Section3 : Principles relating to processing of personal data (Processor)
  - Applies to processors
  - Contracts and subcontracts with controllers, security, transfer of personal data to third countries, etc.

### Procedures

1. Submission of Required Documents and Application
2. Certification audit (ISAE 3000)
3. Determination of eligibility for grant
4. Issue of Certificate

### Time required for Certification (approximately)

N/A

### Renewal and Cancellation

- 3 years (annual audit must be passed)





## 2 dp.mark

### Overview

This is the only certification system to certify that a company is operating based on the rules of TPIPAS (Taiwan Personal Information Protection and Administration System), the only personal data management system promoted by the Taiwanese government. It demonstrates that the business has established an appropriate and adequate management system to comply with PDPA. Certified companies increase confidence in their personal data management capabilities. When combined with CBPR, they can also achieve greater efficiency in complying with cross-border transfer requirements<sup>1</sup>

### Background

The Ministry of Economic Affairs, responsible for establishing personal data protection management system standards and verification system, sought to establish an e-commerce management system and a safe personal data protection environment in accordance with the PDPA revision in 2016. Announced in 2011 to promote TPIPAS management system and create Dp.mark, referring to overseas trends such as Privacy Mark in Japan, TRUTE Mark in US<sup>2</sup>

### Justification Basis

- PDPA (Taiwan)
- OECD, APEC and key GDPR principles on personal data protection requirements

### Details

#### Application/Certification Subject

Businesses based in Taiwan

#### Application/Certification Unit

Corporation

#### Authorization Agency

- Operation: Science and Technology Law Institute (Stili)
- Auditing: 2 bodies

#### Number of Certified Businesses

25 companies

#### Requirements

- The TPIPAS specifications (Taiwan Personal Data Protection and Management System Code<sup>3</sup>) are the standards for certification, including the following items
  - Management responsibility
  - Institutional design
  - Support
  - Implementation of personal data protection management system
  - Improvement
- The Code recommends obtaining international certification (based on CBPR/GDPR) for cross-border transfers (Article 11.12)

#### Procedures

1. Application
2. Application screening by an external authorization agency
3. Document assessment by an external authorization agency
4. On-site assessment by an external authorization agency (visit, interview)
5. Decision and notification
6. Application and use of certification mark

#### Time required for Certification (approximately)

N/A

#### Renewal and Cancellation

- Valid for 2 years (interim audits required after certification)

1. The connection with CBPR is mentioned by TPIPAS (TPIPAS "Shí shī xiào yì [Implementation Benefits]") and by Stili (Stili "TPIPAS shí zhōu nián [TPIPAS 10 years anniversary]")

2. Winkler Partners "DP MARK" 3. TPIPAS "Tái wān gè rén zī liào bǎo hù yǔ guǎn lǐ zhì dù guī fàn 2021 [Taiwan Personal Data Protection and Management System Code: 2021]"

Source: TPIPAS HP





## 3 Data Protection Trust Mark

### Overview

The Data Protection Trust Mark (DPTM) is a voluntary certification program for businesses that aims to foster external trust by promoting and certifying their data protection practices. DPTM allows businesses to demonstrate to customers, business partners, and regulators that they have adopted responsible data protection measures to manage personal data.

If you have ISO/IEC 27001 and 27701 certification, it is relatively easy to obtain DPTM since you have already demonstrated compliance with information security and privacy management standards.

### Background

The Singapore government is promoting its Digital Economy Strategy with the aim of developing the country as a data hub to support international data distribution. As part of this policy, the DPTM system was developed to establish credibility as a data hub and officially started operating in January 2019.<sup>1</sup>

### Justification Basis

PDPA (Singapore)

### Details

#### Application/Certification Subject

The Government of Singapore is committed to the development of Singapore as a data hub supporting international data distribution.

- Organizations that are established or recognized under the laws of the country
- Reside or have an office or place of business in the country

#### Application/Certification Unit

Legal Person/Corporation

#### Authorization Agency

- Operation: IMDA (Information Media Development Authority)
- Auditing: 7 companies. BSI Group Singapore, etc.

### Number of Certified Businesses

118 companies<sup>2</sup>

### Requirements

The certification requirements consist of four principles

- Governance and Transparency  
Appropriate policies and practices, accountability, internal communication and training
- Management of Personal data  
Setting appropriate purposes, providing appropriate notice, obtaining appropriate consent, appropriate use and provision, and compliant cross-border data transfer
- Core of Personal Data  
Enforcement of appropriate protection, proper completion and disposal, accurate and complete records
- Individual's Rights  
Withdrawal of consent, provision of right of access and correction

### Procedures

1. Preliminary evaluation using the DPTM Certification Checklist
2. Submit required documents and application to IMDA
3. Conduct self-assessment according to the self-assessment form provided by IMDA
4. Submit self-assessment and start assessment
5. Assessment (document review, on-site assessment)
6. Completion of assessment and certification decision
7. Issue certificate, mark, etc.

### Time required for Certification (approximately)

N/A

### Renewal and Cancellation

3 years

1. ICOCert "Data Protection Trustmark Certification" 2. IMDA "List of Data Protection Trustmark Certified Organizations (as of 16 Sep 2022)" 2022  
Source: [IMDA "Data Protection Trustmark Certification"](#); ["Data Protection Trustmark Scheme Information Kit" 2022](#)





## 4 Personal Information & Information Security Management System (ISMS-P)

### Overview

Personal Information & Information Security Management System (ISMS-P) is to ensure external reliability of companies' personal data protection and security measures, and to reduce risks of data infringement.

### Background

ISMS-P was established in 2018 as an integrated certification system combining Personal Information Management System (PIMS) and Information Security Management System (ISMS) to eliminate confusion and cost issues.

### Justification Basis

Personal Information Protection Act (Korea)

### Details

#### Application/Certification Subject

<Obligated targets>

- Data communication service provider:
  - Businesses registered under the Telecommunications Business Act (Article 6.1) and serving in “Seoul all major cities”
  - Includes internet providers, internet phones, and mobile communication
- Data communication facility operator
  - Businesses operating and managing integrated facilities for providing information and communication services of others defined in the Network Act (Article 46.1)
- Businesses above a certain size<sup>1</sup>, meeting the standards in the Presidential Decree

<Voluntary applicants>

- All personal data processors (including public/private entities, corporations, associations, and individuals)

**Application/certification unit**  
Corporation

**Authorization Agency**  
Korea Internet & Security Agency (KISA)

**Number of Certified Businesses**  
N/A

#### Requirements

Include 100 items in 3 categories

- Establishment and operation of management system (16 items)
- Management system infrastructure, risk management, etc.
- Requirements for protection measures (64 items)
- Asset management, access control, encryption, etc.
- Requirements in each step of personal information processing (22 items)
- Protection measures when collecting/providing personal information

#### Procedures

1. Establishment and operation of management. system (Minimum 2 months of operation and its evidence)
2. Examination plan and preparation
3. Assessment
4. Decision and notification
5. Issuance of certificate

**Time required for Certification (approximately)**  
N/A

**Renewal and Cancellation**  
Valid for 3 years

1. >150B won annual sales or revenue, or >10B won previous year's sales in IT/communication service sector, or >1M users/day on average in the last 3 months

Source: PIPC "ISMS-P", KISA "ISMS-P in jeung gi jun an nae seo [ISMS-P Certification Criteria]", 2022





## 5 Privacy Mark System

### Overview

The Privacy Mark is a system to evaluate businesses taking appropriate measures to protect personal data, and to allow them to use the mark. It was launched in 1998 to enhance consumers' awareness of personal data protection and to provide incentives for businesses to handle and protect personal data appropriately.

### Background

In the late 1990s, Japan, lagging behind in establishing relevant laws/regulations for personal data protection, established the Guidelines for Protection of Personal Data in 1997 to meet the global standards for personal data protection (esp EU's). However, since the guidelines only indicated global standards of data protection, this system was established to implement/promote protection by businesses handling data. In parallel, the Japanese standard, JIS Q 15001 was also established. The Privacy Mark, in line with JIS, has been revised accordingly to reflect developments in global personal data protection standards (esp GDPR)

### Justification Basis

Guidelines for the Establishment and Operation of the Privacy Mark System

- JIS Q15001

### Details

#### Application/Certification Subject

Businesses with offices in Japan

#### Application/certification unit

Corporation

#### Authorization Agency

- Operation: JIPDEC
- Auditing: 19 bodies including Information Service Industry Association
- Training: 3 bodies including Kansai Information Center (KIC)

#### Number of Certified Businesses

17,154 companies

#### Requirements

- Detailed criteria are available on the JIPDEC website, but at least the following conditions must be met
  - Establishment of personal information protection management system (PMS) complying with JISQ 15001/Guidelines
  - Appropriate handling of personal information with an enforceable system based on PMS
  - PMS must have at least two full-time or registered executive employees in its management
- In addition, implementation of PDCA (Plan-Do-Check-Act) cycle based on management system principles must be done at least once, since records of PMS operation and regulations are required for application

#### Procedures

1. PMS establishment and operation
2. Application/submission of required documents
3. Assessment
4. Certification decision and registration
5. Start using the mark

#### Time required for Certification (approximately)

1 year (4 months for preparation and 6 months for assessment)

#### Renewal and Cancellation

Valid for 2 years





## 6 JAPHIC Mark

### Overview

JAPHIC Mark system is in compliance with APPI/Guidelines to certify businesses establishing and operating a system to take appropriate personal data protection measures. Similar to Privacy Mark, it is widely used in Japan, but acquisition cost and time is less than Privacy Mark, attracting attention from SMEs in recent years

### Background

Along with the establishment of APPI in 2003 and its amendment, the demand for third-party certification of personal data protection systems has been increasing. Although the Privacy Mark system already existed, cost burden (cost/time) was a hurdle for some businesses.

JAPHIC Mark was established as a certification with lower cost and applicable to bidding projects same as Privacy Mark

### Justification Basis

- Act on the Protection of Personal Information
- Guidelines for the Act on the Protection of Personal Information
- Guidelines for the proper handling of specific personal information

### Details

#### Application/Certification Subject

Businesses with offices in Japan

#### Application/certification unit

- Corporation: by corporation or business unit
- Individual: by business

#### Authorization Agency

- Operation: JAPHIC
- Auditing: 3 bodies

### Number of Certified Businesses

359 companies

### Requirements

- JAPHIC publishes details of the assessment criteria in the self-assessment tables. Key items required in each table are as follows
  - Basics of APPI
  - Acquisition of personal data, limitation of purpose of use, outsourcing, measures against leaks, etc.
  - Items related to handling of specific personal data
  - Limitation of use of specified personal data, security control measures, measures against leaks, etc.
- In addition to the above, businesses to which the guidelines for provision to a third party in a foreign country, etc. are applied must also undergo examination based on each guideline

### Procedures

1. Confirmation of application eligibility
2. Self-assessment
3. Web application
4. Assessment by an Authorization Agency (document/on-site assessment)
5. Judgement
6. Issuance of mark/certificate

### Time required for Certification (approximately)

- 1-2months
  - Certification date is the first day of each month after completing assessment

### Renewal and Cancellation

1 year





## 7 EuroPriSe

### Overview

A system that certifies that IT products and IT-based services comply with European data protection regulations. By providing a transparent privacy certificate, EuroPriSe aims to protect consumer and civil rights, provide privacy protection through marketing mechanisms, and ultimately increase trust in IT. As of September 2022, EuroPriSe has not yet been approved by the EDPB as required by the GDPR (Article 42), so the acquisition of EuroPriSe is not proof of compliance with the GDPR, and EuroPriSe GmbH, the operating agency, is aiming to adopt certification by the EDPB.

### Background

It began operating on a trial basis in 2007 under the Data Protection Authority of the German state of Schleswig-Holstein as part of the EU's program to promote the deployment of digital services. Since 2014, EuroPriSe GmbH has overseen management and operation.

### Justification Basis

EuroPriSe Criteria

- Integrate the requirements of the GDPR as well as other European data protection regulations related to data protection, such as the ePrivacy Directive

### Details

#### Application/Certification Subject

Vendors of IT products and IT-related services

#### Application/Certification Unit

Legal Person/Corporation

#### Authorization Agency

EuroPriSe GmbH

#### Number of Certified Businesses

12 companies<sup>1</sup>

#### Requirements

The EuroPriSe Criteria consists of the following four items

- ① Preliminary Issues
  - Purpose of data use, basic technical configuration of the service, etc.
- ② Legitimacy of Data Processing
  - Legal basis for data processing, etc.
- ③ Technical-Organizational Measures
  - Risk assessment of data processing and whether the security level of the subject is appropriate, etc.
- ④ Data Subjects' Rights
  - Obligation to notify, access to/correction of data, etc.

#### Procedures

1. Submit the required documents to apply
2. Sign the contract
3. Examination
4. Grant eligibility determination
5. Issue of Certificate

#### Time required for Certification (approximately)

3-5 months (excluding the applicant's advance preparation period)

#### Renewal and Cancellation

2 years

1. The eTEN program, which ended in 2006 and was taken over by the ICT PSP after 2007 ([European Commission "eTEN programme"](#))

2. Counts the number of companies that are within the validity period on the EuroPriSe HP as of September 2022.

Source: [EuroPriSe GmbH "EuroPriSe Criteria for the certification of IT products and IT-based services \(v2710701\)"; EuroPriSe HP](#)





## 8 TRUSTe Mark

### Overview

The TRUSTe Mark is a system that recognizes compliance with the OECD Privacy Guidelines for eligible websites. While most other certification systems target businesses, this system targets websites and applications for certification. It also has a number of features not found in other certification systems, such as the primary handling of complaints from users by the operating organization and the provision of indemnity insurance. Although the certification system originated in the US, it has a large number of certifications globally, so obtaining certification is useful for fostering global credibility.

### Background

The PC Forum was established in the US in 1997 to promote the healthy development of Internet activities (e-commerce), based on the assertion at the PC Forum in 1996 that "trust is important for the development of e-commerce".

### Justification Basis

OECD Privacy Guideline

### Details

#### Application/Certification Subject (Unit)

Domain, Application

#### Renewal and Cancellation

- Operation: TrustArc
- Auditing: 2 organizations

#### Number of Certified Websites

529 sites

### Requirements

- 19 items regarding the handling of personal data are defined as criteria for review.
  - Restrictions on acquisition, storage, handling of sensitive personal data, etc.
- In the actual examination, the contents of the self-assessment will be verified. The following items are defined in the self-assessment
  - ① Acquisition, use and storage of personal data (Details of personal data to be acquired, etc.)
  - ② Contact to website users
  - ③ How to realize the provision of personal data to third parties
  - ④ Guarantee of accuracy of personal data and reapplication
  - ⑤ Security System
  - ⑥ Personal Data Protection Management (Data Handling Policy)
  - ⑦ Complaint handling

### Procedures

1. Self-assessment
2. Application to Authorization Agency
3. Audit by Authorization Agency
4. Completion of audit and grant of certification (creation of dedicated page, grant of certification mark)

### Time required for Certification (approximately)

2 months

### Renewal and Cancellation

1 year





## 9 CNIL Certification

### Overview

A certification system operated by French data protection authority, CNIL (Commission nationale de l'informatique et des libertés), certifying that adequate safeguards are in place for personal data processing. Certified managers can prove their superiority and reliability in personal data processing. Like EuroPriSe, this certification is not approved by EDPB and is not required to fulfill DPO duties under GDPR. However, CNIL is active in protecting personal data, such as pointing out Megatech's violations of GDPR, and thus its certification is noteworthy.

### Background

Since the time of the EU Data Protection Directive, CNIL has been issuing certification labels to certify the level of personal data protection. After GDPR was enacted in 2018, CNIL changed its certification for DPO (Data Protection Officer) in compliance with GDPR

### Justification Basis

- Data Protection Rules (France)
- GDPR Section 4.4

### Details

#### Application/Certification Subject

- Personal data processors with an office or residence in France, meeting one of the following requirements
  - Professional experience in relevant project/activity (minimum 2 years) and proof of such experience
  - Training on personal data protection (minimum 35 hours)

#### Application/Certification unit

Individual

#### Authorization Agency

- Operation: CNIL
- Auditing: 9 bodies including International Privacy Association of Privacy Professionals

#### Number of Certified Businesses

N/A

#### Requirements

- 17 criteria for DPO certification assessment, including the following items
- Understanding of principles of lawfulness of processing, purpose limitation, data minimization, data accuracy, storage limitation, integrity, confidentiality, and accountability
  - Internal data protection policies or rules
  - Measures against personal data breaches, including notification to supervisory authorities and data subjects
  - Determination of the necessity to perform Data Protection Impact Analysis
  - Training of staff, etc.

#### Procedures

1. Application
2. Pre-screening by an Authorization Agency (screening of application eligibility)
3. Examination
4. Notification of results, issuance of certificate

#### Time required for Certification (approximately)

N/A

#### Renewal and Cancellation

- 3 years
  - Renewal is possible upon retaking the exam at the end of the validity period and upon proof of at least one year of professional experience





## 10 ISMS-PIMS Certification (1/2)

### Overview

A system for evaluating an organization's adaptability to various types of information security assurance mechanisms, based on international standards (ISO/IEC 27701). As the official name "ISO/IEC 27701:2019 Security technology - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines" indicates, it is positioned as an add-on standard (certification)<sup>1</sup> to ISO/IEC 27001 and 27002 as a privacy management standard. Certification allows a company to prove to the outside world that it has a system in place to adequately protect and manage privacy in accordance with global standards. With personal data protection regulations in flux around the world, this international certification is attracting increasing attention as an international certification for privacy management.

Information security standards include ISO/IEC 27000 and 27001, known as the ISO/IEC 27000 series.

ISO/IEC 27701 is one of them and is commonly known as ISMS-PIMS because it is specialized for Privacy Information Management System (PIMS).

### Background

A relatively new certification (standard) issued in August 2019. Even before the birth of ISMS-PIMS certification, it was possible to be personal information protection compliant using ISO/IEC 27002 and 29151. However, both ISO/IEC 27002 and 29151 mainly defined control measures and did not define an operational framework (management system). Therefore, ISO/IEC 27701 was developed as a standard to define a personal information protection management system, and ISMS-PIMS certification was developed as an evaluation system.

### Justification Basis

ISO/IEC 27701

### Details

#### Application/Certification Subject

Managers and/or processors who process personal information<sup>2</sup> within an information security management system

- Organizations of all types and sizes, including public and private companies, government agencies and non-profit organizations

#### Application/Certification Unit

Corporations, Business Units, etc.

#### Authorization Agency

- Operation (Jurisdiction):
  - International Organization for Standardization (ISO)
  - International Electrotechnical Commission (IEC)
- Auditing: External accreditation bodies (many)<sup>3</sup>

#### Number of Certified Businesses

- Japan: 39 companies<sup>4</sup>

1. ISO/IEC 27001 certification (ISMS certification) is a prerequisite (ISO/IEC 27002 certification cannot be a prerequisite because ISO/IEC 27002 does not have an adaptability assessment system and does not function as a certification) 2. "PII (Personally Identifiable Information) 3. List of ISMS-PIMS certification bodies 4. List of ISMS-PIMS certified organizations (as of December 2022)

Source: [ISO "ISO/IEC 27701:2019 Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines"](#)





## 10 ISMS-PIMS Certification (2/2)

### Requirements

- As it is an add-on certification, it basically lists PIMS-specific requirements (additional requirements). In the area of privacy protection, the following standards/regulations are defined in the Annex, as the requirements to be applied are influenced by the organization's situation, national/regional regulations, and other prerequisites.
  - Mapping to the Privacy Framework and Principles defined in ISO/IEC 29100<sup>1</sup> (Annex C)
  - Mapping to GDPR (Annex D)
  - Mapping to ISO/IEC 27018<sup>2</sup> and 29151<sup>3</sup> (Annex E)

### Procedures

- If ISMS certification is already obtained, only the additional requirements are audited.
- If ISMS certification has not yet been obtained, it is possible to obtain ISMS certification at the same time by incorporating it into the ISMS certification acquisition process.

### Time required for Certification (approximately)

- Several months
  - Depends on the status of ISMS certification

### Renewal and Cancellation

- 3 years
  - Since it is an add-on to ISMS certification, it is affected by the expiration date of ISMS certification<sup>4</sup>

1. "ISO/IEC 29100:2011 Information technology - Security technology - Privacy framework 2. ISO/IEC 27018:2019 Information technology - Security technology - Code of practice for the protection of personally identifiable information (PII) in public clouds operating as PII processors" 3. 29151:2017 Information technology - Security technology - Implementation standard for the protection of personally identifiable information" 4. If an organization with an ISMS certification that expires in January 2024 obtains ISMS-PIMS certification in January 2023, the ISMS - PIMS certification will have the same January 2023 expiration date as the ISMS certification.

Source: [ISO "ISO/IEC 27701:2019 Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines"](#)





# 11 Information Security Technology -Personal Information Security Specification

## Overview

Information security technology - Personal information security specification (GB/T 35273-2020) is a national standard that establishes specific handling standards for the processing<sup>1</sup> of personal data by organizations or individuals. Although not legally enforceable, it is an important practical guideline as a national standard that provides general provisions for the handling of personal data protection.<sup>2</sup>

## Background

Issued as a general code for the handling of personal data under CSL, enacted in 2017 (GB/T 35273-1717).

Revised in 2020 due to the growing need after 2019 to add new items adapted to the development of IT technology (GB/T 35273-2020).

The revised version places stricter requirements on personal data managers, including stricter standards for data collection and the additional standards for new business model.

## Justification Basis

N/A

- No applicable laws/standards as this code itself is a standard developed under CSL

## Details

### Application/Certification Subject

Organizations handling personal data

### Authorization Agency

Standardization Administration

### Requirements

- Basic principles for the use and management of personal information. For personal data collection, the requirements include specific situations of use, such as marketing (personalization), etc.
  - Rights of Information subjects
  - Basic principles of personal information security
  - Collection of personal information
  - Storage of personal information
  - Use of personal information
  - Outsourcing, sharing, transfer and disclosure of personal information
  - Incident response
  - Personal information security management requirements of the organization





## 12 JIS Q 15001

### Overview

JIS Q 15001 is a standard that defines the requirements for a management system for organizations to appropriately manage personal data for the purpose of personal data protection. By complying with JIS Q 15001, effective and efficient personal data management can be achieved. In combination with ISO/IEC 27001, a stronger and more effective security management system can be established.

While JIS Q 15001 itself is not a certification but a standard, certification (Privacy Mark) based on JIS Q 15001 is also provided.

### Background

Since the 1980s, international momentum regarding personal data protection, such as the establishment of OECD privacy guidelines and EU data protection directive, led to the launch of P-mark system in 1998. However, because P-mark system was based on guidelines under the jurisdiction of METI, there were concerns that personal data protection effects would be limited to industries under METI's jurisdiction. Therefore, JIS standardization was promoted JIS as a cross-industry effort, and JIS Q 15001 was developed in 1999 (JIS Q 15001:1999). Since there was no comprehensive law on personal data protection in Japan at that time, the standardization was based on guidelines for the protection of personal data in the private sector<sup>1</sup> and the EU data protection directive.

Since then, JIS Q 15001 has revised (JIS Q 15001:2006 and 2017) in response to the enactment and revision of APPI in Japan and international movements (especially GDPR).

### Justification Basis

N/A

- Since JIS Q 15001 itself is a standard, there are no strictly compliant laws/standards
- However, it is consistent with APPI and other management system standards

### Details of the system

#### Application/Certification Subject

Organizations handling personal data

#### Authorization Agency

Japan Quality Assurance Organization (JQA)

#### Requirements

- Defines requirements for establishing a management system for personal data used by the organization
- Provides detailed and specific management items, especially in the annexes
  - Annexes are defined to ensure proximity to ISO<sup>2</sup>

1. From “guidelines for the protection of personal information related to computer processing in the private sector” (1997) (JADAC “JIS Q 15001 kaisei ni itaru keii [Background to the revision of JIS Q 15001],” Information from JADAC and experts No.219 (2018)) 2. In the commentary to JIS Q15001, it is stated that the personal information protection and information security have many common items in term of security control measures, and that the com is aware of the alignment with annex 9L of the ISO supplemental guidelines for the integrated version

Source: JQA “JIS Q 15001 (kojin jouhou hogo) [JIS Q 15001 (personal data protection)]”; JISA “JIS Q 15001 kojin jouhou hogo maneijimento shisutemu youkyuu jikou [JIS Q 15001 personal data protection management system - requirements”





## Other Relevant Tools

The main data protection-related tools used in the countries/regions surveyed

		Title	Country/Region	Applicable laws/Standards	Application/Certification subject
Personal Data Protection 	Certification 	1 GDPR-CARPA	EU (Luxenberg)	GDPR, ISO Standards, etc.	Businesses, Public Organization Other Organizations, etc.
		2 dp.mark	Taiwan	PDPA (Taiwan), Other International Rules, etc.	Businesses
		3 Data Protection Trust Mark (DPTM)	Singapore	PDPA/PDPR (Singapore)	Non-Public Organizations
		4 ISMS-P Certification	South Korea	PIPA (South Korea)	Data Communication Service Providers, etc.
		5 Privacy Mark (P Mark)	Japan	P Mark Operation Guidelines (Compliant JIS Q)	Businesses
		6 JAPHIC Mark	Japan	APPI (Japan), Other Relevant Guidelines	Businesses
		7 EuroPriSe	Germany	EuroPriSe Standards ※Compliant GDPR	IT Product, IT-related Service Vendors
		8 TRUSTe Mark	Global	OECD Privacy Guidelines	Domain, Application
		9 CNIL Certification (Certification des compétences du DPO)	France	EU GDPR, France Data Protection Regulations	Processor of Personal Data
		10 ISMS-PIMS Certification <sup>1</sup>	Global	ISO/IEC 27701	Businesses, Divisions within a business
	Standard 	11 Personal Information Security Specification	China	—	—
		12 JIS Q 15001	Japan	—	—
General Data Protection 	Certification 	1 ISMS Certification <sup>1</sup>	Global	ISO/IEC 27001	Businesses, Divisions within a business
		2 WebTrust	Global	WebTrust Standard	Businesses (Electronic authentication service providers)
	Standard 	3 NIST SP800 Series	US	—	—
		4 SOC2 (Service Organization Control Type2)	US	—	—

1. Some of the ISO/IEC standards have a conformity assessment system. ISO/IEC 27001 and 27701 are classified here as certifications rather than standards because they both have conformity assessment systems.





# 1 ISMS certification (ISO/IEC 27001)

## Overview

SMS certification is a certification system based on international standards (ISO/IEC) that certifies the establishment of a system to ensure the security of various types of information owned by an organization. All information assets owned by an organization are subject to protection, and acquisition of certification proves that the organization has established a data protection system in a wide range of areas.

Certifications related to information security include ISO/IEC 27000 and ISO/IEC27001 within the same ISO/IEC, known as ISO/IEC27000 series. This section introduces ISO/IEC 27001, which deals with requirements related to information security.

## Background

SMS certification is based on BS7799-2 (Information Security Management Systems), a British original standard published in 1999. BS7799-2 was revised in 2002 to incorporate the concept of PDCA to capture international trends in information management, and was partially harmonized with international standards, and adopted/standardized as ISO/IEC27001 in 2005.<sup>1</sup>

## Justification Basis

ISO/IEC 27001

## Details

### Application/Certification Subject

Business units etc. that the business determines to be necessary based on risk assessment concerning information security

### Application/certification unit

Corporations, business units, etc.

### Authorization Agency

- Operation (Jurisdiction): ISO, IEC
- Auditing: External accreditation bodies (many)<sup>2</sup>

### Number of Certified Businesses

- Global: 58,687 companies<sup>3</sup>
- Japan: 6,587 companies<sup>3</sup>

### Requirements

Requirements for information security specifically refer to three elements: “confidentiality”, “integrity”, “ and “availability”

- Confidentiality: information can only be accessed by authorized users
- Integrity: information is stored in an accurate state and cannot be altered or erased
- Availability: information can be accessed by authorized users whenever necessary without any problems

### Procedures

1. Preliminary preparations (select the scope of acquisition, establish the system, etc.)
2. Application for audit
3. 1<sup>st</sup> stage audit (document audit)
4. 2<sup>nd</sup> stage audit (on-site audit)
5. Complete audit and certify

### Time required for Certification (approximately)

Several months

### Renewal and Cancellation

- 3 years
  - Continued examination is required semi-annually to annually during the validity period
  - Renewal examination is required before the end of validity period

1. Nikkei XTECH "Jouhou sekyuritei no shinn kikaku ISO/IEC 27001 wo kaisetsu suru [Explanation of New Information Security Standard ISO/IEC 27001," 2006 2. list of ISMS certification organizations 3. ISO "ISO Survey 2021"

Source: ISO "ISO/IEC 27001 Information Security Management"; JIPDEC "ISMS・ITSMS no hukyu [Spread of ISMS/ITSMS]"; VLC "ISO27001 no gaiyou [Overview of ISO27001]"





## 2 WebTrust

### Overview

WebTrust is an international e-commerce certification program developed in North America. It examines and certifies e-commerce transactions based on international e-commerce assurance standards for Internet businesses. By acquiring WebTrust, businesses issuing various certificates can prove the reliability of the services they provide and operate. Although originating in North America, WebTrust is now being used globally.

### Background

Developed to alleviate consumer concerns about purchasing on the Web as online services become more prevalent<sup>1</sup>

### Justification Basis

N/A

### Details

#### Application/Certification Subject

Companies in all regions

#### Application/Certification Unit

Legal Person/Corporation

#### Authorization Agency

- Operation (Jurisdiction): Chartered Professional Accountants (CPA) Canada<sup>2</sup>
- Auditing: 19 companies certified as Deloitte Equivalent Practitioner<sup>3</sup>

#### Number of Certified Businesses

N/A

### Requirements

- Required criteria vary depending on the services provided by the applicant.
  - Principles and Criteria for CA
  - Principles and Criteria for CA - SSL baseline with Network Security
  - Principles and Criteria for CA - Code Signing Baseline Requirements
  - Principles and Criteria for CA - Extended Validation SSL
  - Principles and Criteria for Verified Mark Certificates
  - Principles and Criteria for Registration Authorities
- The following are the main areas of review<sup>4</sup>
  1. Disclosure of the method of operation  
Disclosure of the method of operation and execution of transactions based on the disclosed information.
  2. Completeness of Service  
Transactions are executed in accordance with the consumer's consent, and a system is in place for accurate billing.
  3. Protection of Information  
A system is in place to protect consumers' personal information from uses not stipulated in the disclosed management scheme.

### Time required for Certification (approximately)

N/A

### Procedures

1. Preparation
2. Audit
3. Certification (Certificate of Guarantee issued)

### Renewal and Cancellation

1 year

1. Journal of Accountancy "In CPAs We Trust" 1997 2. The development of the system was done by the AICPA (American Institute of Certified Public Accountants) and the CICA (Canadian Institute of Chartered Accountants) 3. Counting of the number of businesses published on the CPA Canada HP as of September 2022. 4. GMO Global Sign "WebTrust ni tsuite [WebTrust]"

Source: CPA Canada "WebTrust Seal Program"





### 3 NIST SP800 Series

#### Overview

The Special Publications (SP) 800 series are a set of security guidelines established by US government agencies that cover a wide range of security management, risk management, security techniques, and security measures assessment.

Compared to the SP 800 series, the CSF series is more comprehensive and is therefore used primarily by practitioners.

The SP800 series is subdivided into several sub-series, including SP800-53, SP800-171, and SP800-40<sup>1</sup>.

This section introduces SP800-171, which provides government-recommended security requirements to protect the confidentiality of information and is intended for private operators.

#### Background

With the spread of IT, information security measures have become an important issue not only for the economy but also for national security, as IT has become a critical national infrastructure. Therefore, the US government enacted the Federal Information Security Management Act (FISMA) in 2002, which requires each government agency to develop and strengthen information security. The National Institute of Standards and Technology (NIST) was mandated to assist the federal government in complying with FISMA.

NIST launched a FISMA implementation project in 2003, which led to the establishment of various standards and guidelines, and SP800-171 became effective in 2015 (revised in 2020).

#### Justification Basis

N/A

1. SP800-53 is for government agencies and SP800-40 specifies vulnerability and patch management  
Source: NIST "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations Rev.2" 2021; ManageEngine "NIST hakkou no jouhou sekyuriteli kannrenn bunnsho (CSF to SP80 no ichiduke) [Information Security Documents published by NIST (the position of CSF and SP800)]"

#### Details

##### Target Subject

- All contractors and related companies in the supply chain, from procurement to sales and supply
  - E.g., Head of Systems Development Lifecycle Management, Acquisition or Procurement Responsible for system security risk management and oversight; responsible for security assessment and monitoring

##### Authorization Agency

NIST

##### Requirements

- SP800-171 defines 14 security requirements (Security Requirements for Protecting the Confidentiality of CUI: Security Requirements for Protecting the Confidentiality of CUI in Non-Federal Systems and Organizations)
1. Access Control
  2. Awareness and Training
  3. Audit and Accountability
  4. Configuration Management
  5. Identification and Authentication
  6. Incident Response
  7. Maintenance
  8. Media Protection
  9. Human Security
  10. Physical Protection
  11. Risk Assessment
  12. Security Assessment
  13. System and Communication Protection System and Information Integrity





## 4 SOC2 (Service Organization Control Type2)

### Overview

SOC 2 (Service Organization Controls 2) is one of the AICPA's internal control assurance reports (Service Organization Control Reporting: SOC Reporting) on internal controls and cybersecurity of contractors. It specifically addresses risk controls by external entities.

There are two types of SOC2: Type 1 and Type 2. Type 1 is evaluated as of the base date, while Type 2 is evaluated for a period of time such as one year. As a result of the evaluation, no certification is granted, but the contents of the evaluation are disclosed in a report, which indicates the security control level of the subject.

### Background

In response to a series of massive embellishment scandals in the first half of 2000, the US mandated an assessment of the effectiveness of financial reporting, including internal controls<sup>1</sup>, and the AICPA issued SSAE16 (Statement on Standards for Attestation Engagements No. 16) as its standard for assurance of effectiveness in 2010. In addition, the AICPA developed and published SOC2 as a reporting framework based on SSAE16.

### Justification Basis

N/A

### Details

#### Authorization Agency

AICPA

#### Target Subject

Information system-related businesses (outsourcing providers and their customers, etc.) throughout the world, including the US

#### Requirements

The Trust Service Criteria include the following five criteria, of which security is a mandatory requirement

- Security: protection against unauthorized access
- Availability: overall functionality of the process
- Processing Integrity: appropriateness of processing (completeness, accuracy, timeliness, etc.)
- Confidentiality: protection of information designated as confidential according to the agreement
- Privacy: Adequacy of personal data handling

#### Procedures

The preparation of the report will proceed roughly as follows. Follow the instructions of each audit organization for details.

1. Preliminary Preparation
2. Audit
3. Certification (Certificate of Assurance issued)

SOC2+, which adds optional criteria to SOC2, also exists.

For example, in the US, SOC2+ evaluations with the addition of NIST SP800, etc., are being actively used, and their use is being promoted to meet the needs of operators.

1. Public Company Accounting Reform and Investor Protection Act of 2002 2. SSAE 16 is the standard for financial reporting, and SOC 1 is the standard for internal control over financial reporting.

Source: AICPA "TSP Section 100 2017 Trust Service Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy" 2020; EY "Kuraudo Sekyuriteli ni kannsuru daisannsha hyouka ninshouseido no gaiyou ISO/IEC27017, SOC2 oyobi SOC2+ [Overview of Cloud Security Certification: ISO/IEC27017 certification, SOC2, and SOC2+]," 2016



# Agenda

1. Position of This Project
2. Research related to Cross-Border Data Transfers
- 3. Research on the Actual Utilization by Businesses
4. Summary of Research Results





## 3.1

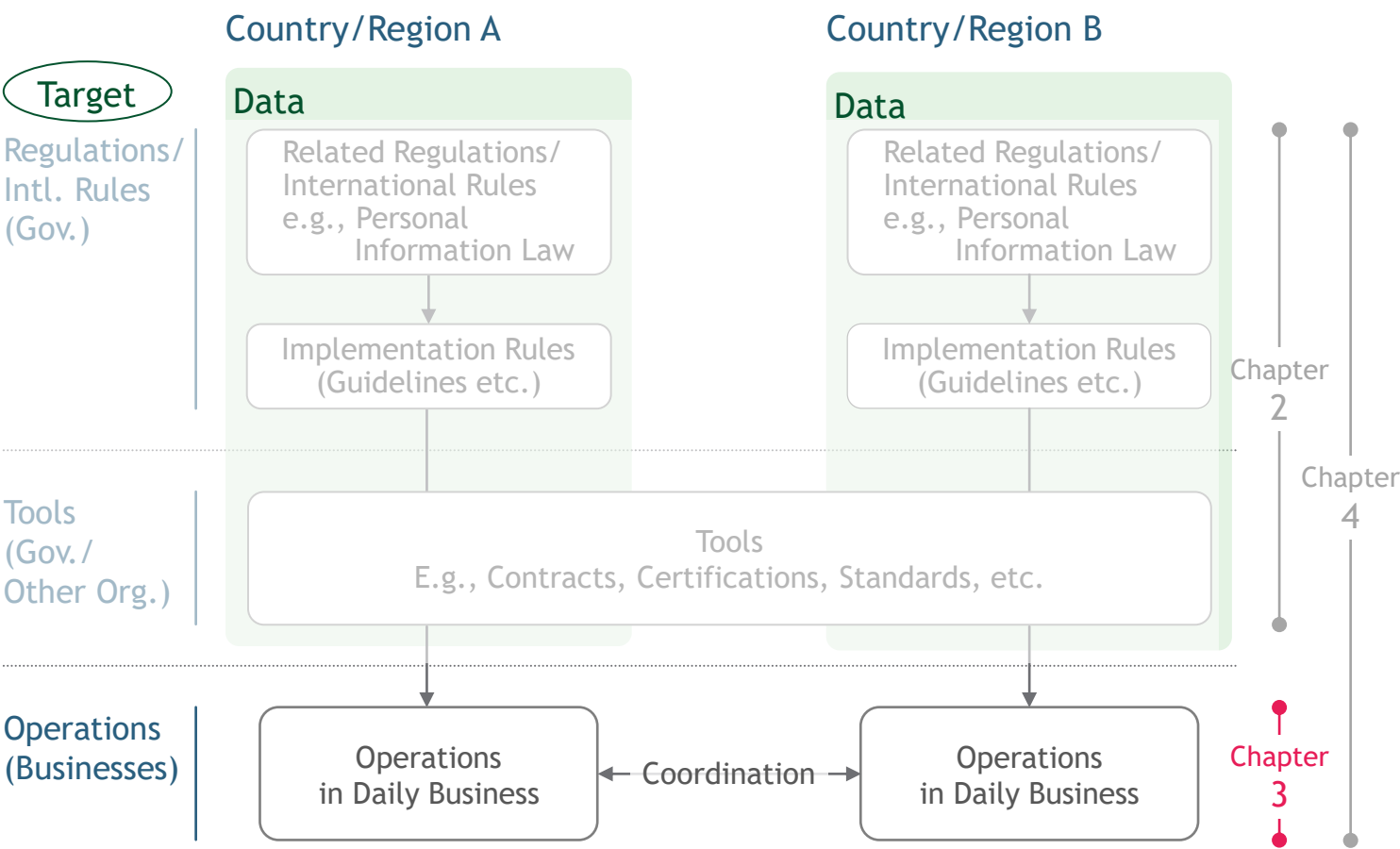
# Research Objectives and Approach



# Objectives of Chapter 3

## Cross-Border Data Transfer Operations

Businesses conduct cross-border data transfer in their daily operations. To carry out transfers, operators implement relevant regulations and utilize tools.



## Objectives

Based on the survey results up to the previous chapter, we will clarify the gap between the actual needs of businesses involved in cross-border data transfers and the current status of regulations/tools for cross-border data transfers.

The survey will be conducted through interviews with operators involved in cross-border data transfers to investigate how they are affected by national/regional regulations and how they utilize each tool in the actual cross-border transfer of data.



Conducted interviews with a total of 16 companies selected to cover a combination of "cross-border data transfer patterns" and "use cases".

### Pattern: 7 Types

#### EU Type: Areas covered by GDPR

- ① EU → Adequacy Decision Countries
- ② EU → Other Regions (SCC/BCR)
- ③ EU → US

#### China Type: Areas with data localization

- ④ China (India/Vietnam) ↔ Others

#### US Type: Areas other than EU and China type

- ⑤ US → Other Countries

#### Multilateral Framework Type:

##### Areas participating in CBPR

- ⑥ Companies within the framework  
→ Companies within the framework
- ⑦ Companies within the framework  
→ Companies outside the framework



### Data Use Cases : 3 Types

#### a) Business Operations

- Assumes personal information of users and information that can be collected by the service
- Including examples of cross-border data crossing to a third country for offshore use

#### b) Research and Development

- Assumes important industrial information such as collected data such as equipment operating data, etc.

#### c) Internal Operations

- Assumes HR data / Global IT governance, etc.



# Companies interviewed for Cross-Border Data Transfer

		(a) Business Operation	(b) R&D (Important Industry Information)	(c) Internal Operation (HR/Groabal IT)
EU Type	① EU → Adequacy Decision Countries	① Internet Service Company ② Railway Company ③ Apparel Manufacturer	⑤ Pharmaceutical Company ⑥ Equipment Manufacturer ⑦ Equipment Manufacturer ⑧ Automotive Parts Manufacturer	⑤ Pharmaceutical Company ⑩ Residential Product Manufacturer ⑪ Consumer Research Firm
	② EU → Other Regions	③ Apparel Manufacturer	-	-
	③ EU → US	-	⑨ US Equipment Manufacturer	-
China Type	④ China (India/Vietnam) ⇔ Others	② Railway Company ③ Apparel Manufacturer	⑥ Equipment Manufacturer	⑤ Pharmaceutical Company ⑩ Consumer Research Firm
US Type	⑤ US → Other Countries	① Internet Service Company ② Railway Company ③ Apparel Manufacturer	⑤ Pharmaceutical Company ⑥ Equipment Manufacturer ⑦ Equipment Manufacturer	⑤ Pharmaceutical Company ⑩ Residential Product Manufacturer ⑪ Consumer Research Firm
Multi framew ork type	⑥ Between Companies within the framework	① Internet Service Company ④ Chinese Game Production	-	⑩ Residential Product Manufacturer ⑪ Consumer Research Firm
	⑦ Companies outside the framework → Companies within the framework	-	⑤ Pharmaceutical Company ⑧ Automotive Parts Manufacturer	⑤ Pharmaceutical Company
Managed by global standards		⑫ Network Equipment Manufacturer ⑬ Internet Service Company ⑭ Cloud Vender ⑮ IT Company ⑯ Internet Service Company	-	-



# Hearing items related to business needs and gaps

Category	Hearing Questions
<b>Confirmation of assumptions</b> <ul style="list-style-type: none"> <li>Relevant regulations/ cross-border data</li> </ul>	<p>In which countries and regions are cross-border data transfers occurring?</p> <p>Where and how is the data stored in each country?</p> <p>What is the intended use of each data and who are the users and use cases?</p> <p>What regulations apply to each data regarding cross-border data transfers?</p> <p>What are the cross-border data categories (marketing/HR/R&amp;D) and items?</p>
<b>Compliance with each regulation</b> <ul style="list-style-type: none"> <li>Tools to be used etc.</li> </ul>	<p>How do you comply with privacy regulations in each country?</p> <p>What tools are currently in use? (Check European/US type, other country framework type)</p> <p>Why do you use those tools? How was the response policy formulated?</p> <p>What are the benefits of the current tools and their use?</p> <p>What are issues and points for improvement regarding the current tools and their use?</p> <ul style="list-style-type: none"> <li>“We gave up the business due to a lack of tools that can be used in the first place and an inability to send cross-border data”</li> <li>“Cost and time required to support and research tools are a burden”, “Low predictability”, etc.</li> </ul> <p>What factors (industry rules, etc.) other than tools impact data protection and how are they being addressed?</p>
<b>Ideal data distribution</b>	<p>What kind of business opportunities will open up if cross-border DFFT is realized based on certain criteria/hurdles?</p> <p>In what regions/data would this be particularly important?</p>
<b>*Items to be confirmed for the companies including data transfer to China</b>	<p>Which countries/regions (check China type) are obligated to store data domestically due to business relations?</p> <p>What data types and categories are subject to domestic retention obligations?</p> <p>Where and how is data stored in each country (on-premise/cloud?)? What are the data storage locations and storage methods (on-premise/cloud?) in each country?</p> <p>How do local operations and use cases for each data differ between countries with in-country storage obligations and the rest of the world?</p> <p>What are the points that need particularly urgent improvement in business relationships?</p>





## 3.2

# Summary of the Results



# Overview of Business Needs

Each business decides on the tool according to its own data transfer needs/scope. They are dissatisfied with the cost of implementation and the lack of predictability



## Business chooses the scope of transfer; whether they want to transfer data to outside the group or not

- WANT to transfer data to companies outside the group:
  - Use SCC/MCC. Businesses need to make different contracts according to each situation.
- DO NOT WANT to transfer data to companies outside the group:
  - WANT to build universal data governance: Use BCR
  - DO NOT WANT to build universal data governance: Use SCC
  - Low Risk: Obtain the consent of data subject



## Businesses use CBPR certification to obtain credibility

- Businesses want to establish a global system that includes data transfer to companies outside the group



## Businesses are concerned about...

- TOO MANY REGULATIONS "It's difficult to decide on the most appropriate tool considering the differences between regulations"
- TOO MUCH COST "We spent billions of yen on research",  
"It required a lot of time and human resources for coordination"
- LOW PREDICTABILITY "We have no choice but to interpret it strictly due to its unclear legal interpretation"



# Company Needs/Issues and Benefits of Implementing Each Cross-Border Tool

Tool	Company (data)	Comment
BCR	Cloud Vender (Personal data in SaaS)	<ul style="list-style-type: none"> <li>Customer data in one country's data center may be accessed by a team in another country for the purpose of providing SaaS services</li> <li>We want common global data cross-border rules for SaaS service operations in anticipation of data cross-border cases</li> </ul>
	Internet Service Company (EC customer data, etc.)	<ul style="list-style-type: none"> <li>The company adopted BCR to promote and gain trust in the data management system of the company's PF service</li> <li>Each branch office has a qualified attorney who checks laws and regulations and the current situation in each country to ensure uniform data governance on a global basis</li> </ul>
SCC	Pharmaceutical Company (Medical records, safety information, internal HR data)	<ul style="list-style-type: none"> <li>SCC was adopted to avoid BCR, which has unclear criteria and risks dismissal of the application</li> <li>Because of the large number of group companies, it took time to handle the signing of the SCC                             <ul style="list-style-type: none"> <li>It was necessary to conclude an SCC contract with all group companies to realize the integration of HR data</li> <li>It took time to get smaller group companies to understand the need for SCC</li> </ul> </li> </ul>
CBPR	IT Company/ Network Equipment Company (Company internal data)	<ul style="list-style-type: none"> <li>Companies can demonstrate that they have the processes and technology to confirm that they are following the CBPR framework and guidelines, which will lead to client trust                             <ul style="list-style-type: none"> <li>Image similar to ISO and NIST</li> </ul> </li> <li>CBPR does not support California/New York state law and is not legally binding like GDPR. It is necessary to invest money and time in CBPR compliance (certification and updates)</li> </ul>
	Internet Service Company (EC customer data, etc.)	<ul style="list-style-type: none"> <li>We avoided the less predictable BCR and opted for SCC.</li> <li>CBPR is expected to be extended (e.g., the shortfalls in the data governance systems of Company A and Company B will be addressed by both A and B and joined across borders for a specific purpose)                             <ul style="list-style-type: none"> <li>SCC is purpose-specific (e.g., multiple SCCs b/w Companies A and B by data type and purpose of use)</li> <li>Non-APEC expansion is also expected. Middle East and Africa are waiting for the non-EU framework</li> </ul> </li> </ul>



# Cross-Border Transfer Needs and Tools utilized by Companies interviewed (1/2)

Data Transfer Needs	Data Transfer Tools	Company
Transfer outside the group	<p><b>A</b> Establish universal data governance N/A (There is a need but no tool to address it)</p> <p><b>B</b> Comply with regulations on a case-by-case basis SCC/MCC and other business contracts</p>	<p>N/A</p> <p><b>2</b> Railway Company (Data via local company) <b>4</b> Chinese Game Production (Data outside of China) <b>6</b> Equipment Manufacturer <b>13</b> Internet Service Company</p>
Transfer within the group	<p><b>C</b> Establish universal data governance BCR</p> <p><b>D</b> Comply with regulations on a case-by-case basis SCC/MCC and other business contracts</p> <p>Establish internal rules for personal data management and voluntarily respond to risks without using existing tools</p> <p><b>D</b> Minimum Response (Low Risk) Adequate decision + Consent of the data subject Consent of the data subject</p>	<p><b>1</b> Internet Service Company <b>12</b> Cloud Vender <b>14</b> Network Equipment Manufacturer</p> <p><b>5</b> Pharmaceutical Company <b>9</b> US Equipment Manufacturer <b>10</b> Residential Product Manufacturer <b>13</b> Internet Service Company</p> <p><b>1</b> Internet Service Company</p> <p><b>7</b> Equipment Manufacturer <b>3</b> Apparel Manufacturer</p> <p><b>2</b> Railway Company (Data collected directly from users) <b>11</b> Consumer Research Firm</p>
Common for both	<b>E</b> Gain External Credibility CBPR certification	<p><b>12</b> Network Equipment Manufacturer <b>13</b> Internet Service Company <b>15</b> IT Company <b>16</b> Internet Service Company</p>
<b>F</b> Abandoned (The need for data transfer exists)	N/A	<p><b>3</b> Apparel Manufacturer (Developed app exclusively for China) <b>5</b> Pharmaceutical Company (Used data only in China/abandoned global use) <b>6</b> Equipment Manufacturer (Handled by local agency) <b>8</b> Automotive Parts Manufacturer (Collected masking data only)</p>



# Cross-Border Transfer Needs and Tools utilized by Companies interviewed (2/2)

Data Transfer Needs		Data Transfer Tools	
Transfer outside the group	A Establish universal data governance	Companies want to establish universal data governance, including companies outside the group (But there is no appropriate tool)	
	B Comply with regulations on a case-by-case basis	Cross-border data transfer with companies outside the group can only be handled through inter-company agreements such as SCC, etc. Therefore, companies should create specific contracts according to the regulations of the target countries	
Transfer within the group	C Establish universal data governance	When companies expect to have many corporates/customers as platform providers (such as global cloud providers, etc.), BCR helps gain external credibility	
	D Comply with regulations on a case-by-case basis	Since the acquisition of a BCR costs billions of yen, many companies choose to enter into SCCs and other inter-company agreements among group companies	
	D' Minimum Response (Low Risk)	In cases where the possibility of litigation or the risk of sanctions is low (e.g., handling only employee data), it is possible to reduce costs by only obtaining data handling consent from the data subject	
Common for both	E Gain External Credibility	Currently, the CBPR is used more as a means of gaining customer confidence in data governance systems than as a means of complying with national laws and regulations	
F Abandoned (The need for data transfer exists)		In principle, the transfer of personal information and critical industry data (including geographic data) is not allowed in China, so some companies have abandoned the idea of transferring data across the border even though they have cross-border needs	

On the other hand, companies can also select other tools (such as SCC and BCR) for cross-border transfers within a group.

In addition, when the risk of sanctions is estimated to be low, there is a pattern of only obtaining the consent of the data subject.



# Cross-border transfer needs and tools by data processed (general trends)

		End-user attribute/biz data on cloud/network services, and personnel data within group <sup>1</sup>		B2B customer data, R&D data, and personnel data within group <sup>1</sup>		B2C customer data, personnel data within group <sup>1</sup>	
Cross-border transfer needs (purpose)		<b>C</b> Cross-border transfers, incl. within and outside the group > Gain trust in data governance	<b>E</b> Cross-border transfers within the group > Collectively establish common global data governance	<b>B</b> Cross-border transfers outside the group > Handle individual country/region regulations <b>D</b> Cross-border transfers within group > Handle individual country/region regulations		<b>D</b> Cross-border transfers outside the group > Handle individual country/region regulation > Handle minimal (sanction risk: low)	
Cross-border tools:		✓	✓	✓		✓	✓
Tool summary	Detail	<b>CBPR</b> <ul style="list-style-type: none"><li>Personal data protection certification to enable cross-border transfers within member countries</li><li>Required personal data protection sys. is established, and cert. is obtained after an audit</li><li>Clear/specific requirements (criteria and application items) are set forth for the cert. sys.</li></ul>	<b>BCR</b> <ul style="list-style-type: none"><li>Personal data protection policy to allow cross-border transfer between group coms</li><li>Use requires an in-house data protection policy and approval from the responsible authorities</li><li>No model is available, only an overview of requirements in each country/region</li></ul>	<b>SCC/MCC</b> <ul style="list-style-type: none"><li>Contracts between data exporters/importers for cross-border transfers</li><li>A model is available, and the requirements for cross-border transfers are comprehensive/specific</li><li>Increased adoption, incl. by regional organizations such as EU, ASEAN/Ibero-America, etc.</li></ul>		<b>Adequacy decision</b> <ul style="list-style-type: none"><li>A system that allows target countries the same level of protection as their own country/region</li></ul>	<b>Consent</b> <ul style="list-style-type: none"><li>A system to obtain the consent after notifying the reason and purpose of cross-border transfer</li><li>Adopted by many regulations</li></ul>
	Acquisition difficulty	★★★★★ If in-house personal data protection systems are required, but relevant cert. (e.g., P mark) have been obtained, lower cost/difficulty to handle	★★★★★ Based on regulatory requirements, need to develop a common personal data protection for the group. Higher cost/difficulty to handle as approval application is also required	★★★★★ SCC/MCC are less costly/difficult to handle due to standardized contract clauses		★★★★★ Considerably low cost/difficulty, as the terms of use and obtaining the consent of user can be done within in-house services	
Summary of hearing results		<ul style="list-style-type: none"><li>Many operators <b>are not recognized or do not understand the details of CBPR</b> (10/16 companies)</li><li>Of those that are properly recognizing CBPR (6 companies), 4 companies acquired CBPR<ul style="list-style-type: none"><li>However, majority of operators obtained for the purpose of gaining external credibility rather than for cross-border transfer itself</li><li>Understand the benefits of CBPR and <b>expect CBPR to be expanded in future</b><ul style="list-style-type: none"><li>Expand no. of adopting countries</li><li>The US (No comprehensive law, need to check state laws; expect consolidation with CBPR)</li></ul></li></ul></li></ul>	<ul style="list-style-type: none"><li>All operators recognize SCC (16/16 companies). But only 3 companies have acquired BCR<ul style="list-style-type: none"><li>Acquisition hurdles are high, and many have not yet adopted it<ul style="list-style-type: none"><li>Only within a group of coms</li><li>No standard format exists</li><li>Full governance for all group coms is difficult and the risk of BCR violations is hard to avoid</li></ul></li><li>Companies that do not have a fixed data storage location or purpose of use for their users like cloud services and that want to provide services globally adopt BCR</li></ul></li></ul>	<ul style="list-style-type: none"><li>All operators recognize SCC (16/16 companies). About half of them chose SCC/MCC (7/16 companies)<ul style="list-style-type: none"><li>Widely used because the contract format is standardized and only a com-to-com contract is required</li><li>But multiple SCCs are required in some cases depending on the type of data and purpose of use, which can be costly for global companies</li></ul></li></ul>		<ul style="list-style-type: none"><li>Can be completed only by consent within in-house services, but there is a burden to deal with GDPR compliance<ul style="list-style-type: none"><li>Need to set up CDO, ensure sufficient capacity to respond to user rights, and create SLAs regarding the timing of data deletion, etc.</li><li>Age of consent varies from 13 to 16 even within Europe</li></ul></li></ul>	

1. Hearing 10 applies to cross-border transfers of intra-group personnel data. Other operators, excl. 10, also perform cross-border transfers of personnel data, but the transfers are performed using the cross-border transfer tool used by the main business





## 3.3

# Details of the Results: Business Interviews



# 1 Internet Service Company

Selected BCR because cross-border transfers within the group are the focus, and aim to gain customer trust by achieving common global data governance

## Company/Business Overview

### Company overview

- Industry: EC business, telecommunications business

## Cross-Border Data Transfer Needs

Data subject	Data type	Purpose of use
Customer information	<ul style="list-style-type: none"><li>• Name</li><li>• Address</li><li>• Phone no.</li><li>• Frequency of service use</li></ul>	Digital marketing (CRM, WebAds, etc.)

## Regulatory Compliance Method

- Selected Tool**
- BCRs are required by group's main subsidiaries and some joint ventures to enable cross-border transfer
    - Cross-border transfer of group data to a dev. center in China is also possible
    - Since biz partners and contractors are not covered by BCR, processed by the department in charge of information privacy and governance or by a lawyer qualified in each country

- Reasons/ Process of Tool Selection**
- Decided on a policy to achieve standard data governance globally and obtain BCR when GDPR was enforced in 2017
    - Selected BCR with the aim of gaining customer trust in order to penetrate platform services overseas in future. Invested billions of yen in global data governance
  - HQ team in country A and staff qualified as lawyers at branch offices in each country responded
    - Focus on developing a system to obtain BCR and ISMS certification without allocating resources to SCC conclusion etc.
    - Also, established a common data governance policy globally
  - As a result, succeeded in obtaining BCR in about 2.5 yrs.

- Barriers/Needs in Tool Usage**
- As low-stake joint ventures are difficult to include in BCR framework because of governance issues, dealing with the need for cross-border transfers is challenging

- Comments on CBPR**
- CBPR is difficult to penetrate the market for 3 reasons: ① it is difficult for coms to understand the benefits of applying data in a manner different from GDPR, ② there is only a small no. of target countries/coms with CBPR certification, ③ it is necessary to reapply for certification every year
    - ① Difficult to imagine how DFFT will expand business opportunities
    - ② System is that if the no. of coms that obtain the certification is small, the benefits of obtaining it is also small. So, if companies that operate IT businesses on a large scale, such as platformers, do not obtain CBPR first, other companies will not follow suit (especially SMEs).
    - ③ Security tools are generally updated every few years and it requires report the difference in efforts since the last update, but CBPR appears to be a high hurdle as it seems to be reviewed annually on a zero-based instead of updated
  - For DFFT to be developed, it is expected that tools be easy for coms to use and that they are both offensive and defensive

## Flow of Cross-Border Data Transfer and Tools Used

Each data is stored in the region and data analysis is performed by the region manager, but cross-border data transfer is required to make the data available for viewing by the HQ in country A.

① Europe, Country B/C ⇄ Country A (head office location): BCR



## 2 Railway Company: Reservation Function

The company selected SCC since cross-border transfer was needed with companies outside the group, but handled the data of other nations collected directly by the group with consent from users

Company/Business Overview	Cross-Border Data Transfer Needs (ticket reservation business only)		
Company overview <ul style="list-style-type: none"><li>Business type: railway</li></ul>	Data subject	Data type	Purpose of use
	User	Name / address / passport no. / billing address	Ticket reservation and payment settlement
Ticket reservation biz for tourists visiting Japan <ul style="list-style-type: none"><li>Deployed in Europe/US/China/Country B</li></ul>			

### Flow of Cross-Border Data Transfer and Tools Used

The data are all consolidated into the data server in Country A

① Europe → Country A : SCC or GDPR-compliant privacy policy

② US / China / Country B → Country A : Minimum privacy policy

### Regulatory Compliance Method

Selected Tool	<ul style="list-style-type: none"><li>① Europe → Country A<ul style="list-style-type: none"><li>For reservations through local travel agents in EU, conclude SCC with travel agents to realize cross-border data transfer</li><li>For individual online reservations, present GDPR-compliant privacy policy and obtain consent for the use of personal information on website</li><li>Continue the above response before/after the adequacy decision</li></ul></li><li>② China / US / Country B → Country A<ul style="list-style-type: none"><li>Present a privacy policy and obtain consent on the use of personal information</li></ul></li></ul>
Reasons/Process of Tool Selection	<ul style="list-style-type: none"><li>Chose SCC in line with EU regulations as sanction risks are greater in EU where core businesses are based</li><li>Support for China / US / Country B is kept at minimum basis<ul style="list-style-type: none"><li>China: No main business base, less risk than Europe in case of sanctions</li><li>US and B countries: Less likely to be sanctioned than Europe and China</li></ul></li></ul>
Barriers/Needs in Tool Usage	<ul style="list-style-type: none"><li>Since it was before an adequacy decision was obtained, the biggest hurdle was the cost of tens of millions of orders to perform research for GDPR support, conclude SCC, and to develop GDPR-compliant privacy policy<ul style="list-style-type: none"><li>Legal department used substantial resources to create a format for privacy policy using external consultant (to interview local data usage, etc.)</li><li>Though SCC had an established format, the company needed to support the travel agents and the contract partner to cover their poor legal capabilities.</li></ul></li><li>There are needs for clarifying and interpreting regulations and for presenting support methods<ul style="list-style-type: none"><li>"Local EU coms interpreted GDPR optimistically within the reasonable range, but coms in Country A had no choice but to make strict interpretations out of concerns for sanctions"</li><li>"Want to know clearly how sensitive we need to respond to each use case"</li></ul></li></ul>

Comments on CBPR	(Not mentioned)
------------------	-----------------



### 3 Apparel Company: SNS Operations Overseas

Due to the low risk of sanctions for cross-border transfers, the company chose to accept GDPR adequacy decision and a GDPR-compliant privacy policy

Company/Business Overview	Cross-Border Data Transfer Needs (SNS business only)		
<b>Company overview</b> <ul style="list-style-type: none"> <li>Business type: Apparel</li> </ul>	Data subject	Data type	Purpose of use
<b>Fashion SNS business</b> <ul style="list-style-type: none"> <li>Released in 2020</li> <li>Deployed in Country A/US/EU/China</li> </ul>	User	Posted photo	Browsing by users in other countries Off-shore data censorship
	Employee (Store staff)	Posted photo Name Name of the store	

#### Flow of Cross-Border Data Transfer and Tools Used

① Europe → Country A : GDPR adequacy decision + GDPR-compliant privacy policy
② US → Country A : CCPA-compliant privacy policy
③ Country A → EU/US : GDPR-level privacy policy
④ Country A → Philippines : GDPR-level privacy policy (Consent to re-transfer using ext. vendor)
⑤ China → Country A: dropped (use a domestic server in China)

#### Regulatory Compliance Method

Selected Tool	<ul style="list-style-type: none"> <li>① Europe → Country A <ul style="list-style-type: none"> <li>Use GDPR adequacy decision for data consolidation to Country A. Obtain consent from users on GDPR-compliant privacy policy.</li> </ul> </li> <li>② US → Country A <ul style="list-style-type: none"> <li>Considering the burden of identifying posts by California State residents and risks when the regulation is updated, present CCPA-compliant privacy policy in the entire US and obtain permission from the users.</li> </ul> </li> <li>③ Country A → Europe / US <ul style="list-style-type: none"> <li>Transfer the data consolidated in Country A to the third country, present the location /usage of the data and obtain permission</li> </ul> </li> <li>④ Country A → Philippines <ul style="list-style-type: none"> <li>The Philippines does not obtain EU adequacy decision, they outsource to vendors by notifying users of the possibility of data transfer when obtaining their consent on the privacy policy</li> </ul> </li> <li>⑤ China → Country A <ul style="list-style-type: none"> <li>Dropped cross-border data transfer due to the difficulty of obtaining data security transfer evaluation. Join hands with Tencent to launch service using the data server in China</li> </ul> </li> </ul>
Reasons/Process of Tool Selection	<ul style="list-style-type: none"> <li>For applications shared by Country A, Europe, and the US, the company created rules based on GDPR, which is the most stringent of Country A's personal information protection law, Europe's GDPR, and the US CCPA, and chose a policy of additional local support.</li> <li>For China, in light of the risk of sanctions due to data crossing borders, the company created an app closed to China in cooperation with a local subsidiary.</li> </ul>
Barriers/Needs in Tool Usage	<ul style="list-style-type: none"> <li>Even with adequacy decision, support for GDPR-compliance is still time-consuming <ul style="list-style-type: none"> <li>CDO (Chief Digital Officer) assignment, support for user rights, SLA (Service Level Agreement) for data deletion timing are required</li> </ul> </li> <li>To use an offshore company as an outsourced vendor, the company must be responsible for managing and monitoring the security of the vendor</li> <li>The company wishes to reduce the burden of determining the differences in individual rules for each country on a case-by-case basis as a company.</li> <li>The company wishes to establish uniform rules not only for the handling of personal information, but also for age restrictions (age at which users can consent to a contract) when obtaining permission from users. <ul style="list-style-type: none"> <li>The age of consent varies from 13 to 16 years old even within the EU</li> </ul> </li> </ul>

Comments on CBPR	(Not mentioned)
------------------	-----------------



## 4 China Game Production Company

The company selected SCC because it requires cross-border transfers with firms both inside and outside the group

### Company/Business Overview

#### Company overview

- Business type: game production
- Leading game company in China, and develops services in Asia and Europe
- Has subsidiaries / joint companies in each country

### Cross-Border Data Transfer Needs

Data subject	Data type	Purpose of use
User	<ul style="list-style-type: none"><li>• User ID</li><li>• Hardware device ID, etc.</li></ul>	<ul style="list-style-type: none"><li>• Competition in games with users of other countries</li><li>• Analysis for ad &amp; marketing</li></ul>

### Regulatory Compliance Method

#### Selected Tool

- Obtain permission for data usage from the users when they join the game PF
- Conclude SCC among companies that need cross-border data transfer
  - E.g.: Between a data management. operator (Gr com) in Singapore and Ad/gaming operation com in Country A (joint company)
  - E.g.: Between own company and a development lab in the US
- The answer was not given on the actual data cross-border in China

### Flow of Cross-Border Data Transfer and Tools Used

Consolidate the data of Asian users in the servers either in Singapore or Hong Kong

- Not using the server in China because communication speed could not be secured for users outside China due to firewall and because complaints were given from the users

Similarly, consolidate the data of EU users in the server in Europe

- ① Several countries incl. Country A → consolidate in the server either in Singapore or Hong Kong:  
Conclude a consent for data usage between employees and companies to obtain permission for data collection  
(No clear answer given on other data cross-border flow)

#### Reasons/Process of Tool Selection

- The China HQ legal department and a data privacy officer (lawyer) for each business unit discussed how to select tool

#### Barriers/Needs in Tool Usage

- From the perspective of Chinese companies, GDPR and other overseas regulations do not have clear data protection criteria or handling methods
  - "Chinese regulations are easier to understand with clear requirements. GDPR is unclear on practical requirements"
- It is ideal to use a common framework globally, but that is not realistic. If less restrictive framework was established outside Europe, business opportunities would increase

#### Comments on CBPR

(Not mentioned)



## 5 Pharmaceutical Company

The company chose SCC due to unclear BCR criteria regarding cross-border transfers with companies within the Group

### Company/Business Overview

#### Company overview

- Business type: pharmaceutical
- Nearly 200 group companies inside / outside the country

### Cross-Border Data Transfer Needs

- ① Chart information for clinical development
  - Name address, age, drug use history, efficacy, disease history, etc.
  - Pseudonymized, but is considered sensitive personal information
- ② OTC drugs safety information (reporting obligation to government)
  - Information includes drug combinations, side effects (blood pressure readings, etc.), and doctors' knowledge, and thus constitutes personal information requiring special consideration.
  - In addition, information on devices such as syringes, etc., is also retained to provide compensation for damages in the event of an incident.
- ③ Internal HR data
  - Employees' name, gender, address, background, etc.

### Regulatory Compliance Method

#### Selected Tool

- Europe / Country B / Country C, etc. ⇔ Country A
- Uses SCC without taking risks, as application for BCR was said to be turned down due to unclear criteria

#### Reasons/Process of Tool Selection

- Privacy officers exist in all three locations (Europe, Country B, Country C), and discussions take place among the three and the legal department
- Uses consulting firm such as PWC and KPMG for GDPR-compliant project management. Also requests several law firms for support
- Concludes SCC with HQ and each Gr com individually
  - Concludes SCC after carefully conducting impact assessment and security audit
  - Gives privacy notice to the data subject
  - Uses the same tool to support data cross-border needs ①②③
- Having nearly 200 Group companies, prioritization is determined based on cross-border data transfer needs
  - Not all Group companies handle cross-border data transfer needs ①②, but needed to conclude SCC with all Group companies to achieve ③
  - Started discussion in 2017 and completed SCC handling in 2020

#### Barriers/Needs in Tool Usage

- Smaller-sized Gr coms did not easily understand the need of SCC and it took time to persuade them
  - They persistently questioned if there were easier electronic approval methods than SCC
- As a result, information was shared but SCC was not concluded for some time
- Positive about regulations that promote data distribution
  - "There is no point of just collecting the data. If safe usage of the data is realized through the regulations as with the personal information protection law in Country A, regulations rather support the distribution of the data"

#### Comments on CBPR

(Not mentioned)

### Flow of Cross-Border Data Transfer and Tools Used

- ① Europe / Country B / Country C, etc. ⇔ Country A : SCC + privacy notice
- ② China → Country A: dropped (use a domestic server in China)



## 6 Equipment Manufacturer

Selected SCC as cross-border with companies outside the Group is required

### Company/Business Overview

#### Company overview

- Business type: construction manufacturer
- No. of sales base abroad: 54

### Cross-Border Data Transfer Needs

Data subject	Data type	Purpose of use
User	<ul style="list-style-type: none"> <li>• Location</li> <li>• Operation</li> <li>• Fuel consumption</li> <li>• Wear info</li> </ul>	<ul style="list-style-type: none"> <li>• Research &amp; development</li> </ul>

### Regulatory Compliance Method

#### Selected Tool

Europe ⇔ Country A

- Concludes SCC with a sales destination company. A separate consent for data usage is also obtained at time of sales contract

China ⇒ Country A

- Dropped

#### Reasons/Process of Tool Selection

- When entering the Chinese market, the company was instructed by the Chinese authorities that cross-border use of data was prohibited and decided against using the data
- Local entity conducts primary processing of data analysis / masking

#### Barriers/Needs in Tool Usage

- In China, geographic information is masked, so it is impossible to grasp which regions and for what purposes the data is being used, and the strategic policy for China is left up to the sales companies. Therefore, upper management at the HQ in Country A is concerned about whether the Chinese sales companies are utilizing the data correctly.

#### Comments on CBPR

(Not mentioned)

### Flow of Cross-Border Data Transfer and Tools Used

Consolidate the data of the Europe / US into an on-premise server at HQ in Country A

Domestic data in China is managed w/ the server of local entity in CN

- ① Europe → Country A : SCC + consent for data usage at time of sales contract
- ② US → Country A: Consent for data usage at time of sales contract
- ③ China → Country A: dropped (use a domestic server in China)



## 7 Equipment Manufacturer (as of 2020)

The company envisions data cross-border using GDPR sufficiency certification due to low risk of sanctions from cross-border transfers

### Company/Business Overview

#### Company overview

- Business type: equipment manufacturer
- No. of bases abroad: 53

### Cross-Border Data Transfer Needs

Data subject	Data type	Purpose of use
User	<ul style="list-style-type: none"> <li>• Location</li> <li>• Operation</li> <li>• Fuel consumption</li> <li>• Wear info</li> </ul>	<ul style="list-style-type: none"> <li>• Research &amp; development</li> </ul>

### Regulatory Compliance Method

#### Selected Tool

Europe ⇒ Country A

- Data collection within EU and cross-border data transfer relies on the security policy of the cloud server + GDPR + adequacy decision (cross-border data transfer is not started as of 2020)

US ⇒ Country A

- Due to detailed industry regulations, priority is given to industry regulations regarding collected items and handling of personal data (cross-border data transfers have not yet been reviewed)

China ⇒ Country A

- Decided against data access to China due to three data protection regulations in China and industry regulations

### Flow of Cross-Border Data Transfer and Tools Used

The data of EU, US are managed by local cloud server

The data of sales outlet in China are managed by local entity server

<Cross-border transfer has not started in 2020 (only planning)>

- ① Europe → Country A: relies on the security policy of cloud server + GDPR + adequacy decision
- ② US → Country A: Give priority to responding to industry regulations (data cross-border is not discussed)
- ③ China → Country A: dropped (use a domestic server in China)

#### Reasons/Process of Tool Selection

- The legal department at the HQ in Country A does not have the ability to collect information on the laws and regulations of each country and responds upon request from business divisions.

#### Barriers/Needs in Tool Usage

- As employees of Country A are assigned to the overseas sales outlet as executives, it is difficult for them to get into each group and gather information due to language and relationship barriers
- Therefore, they tend to lag behind in product development in line with the regulations

#### Comments on CBPR

(Not mentioned)



## 8 Automotive Manufacturer

As there is no need for personal information items, the company chooses cross-border data transfers with masked data except for the portions necessary for the analysis

Company/Business Overview	Cross-Border Data Transfer Needs (connected car business only)			Regulatory Compliance Method	
<b>Company overview</b> <ul style="list-style-type: none"> <li>Business type: automotive manufacturer</li> <li>36 bases inside / outside the country</li> </ul>	Data subject	Data type	Purpose of use	Selected Tool	① Europe → Country A <ul style="list-style-type: none"> <li>Shares masked secondary data with Country A</li> </ul> ② Thailand, Country B, Country C → Country A <ul style="list-style-type: none"> <li>Shares masked secondary data with Country A</li> </ul>
	User	<ul style="list-style-type: none"> <li>Location</li> <li>Fleet no.</li> <li>Car type</li> <li>Name of contractor</li> <li>Address of contractor</li> </ul>	<ul style="list-style-type: none"> <li>Research &amp; development</li> <li>Data is masked for usage</li> </ul>	Reasons/Process of Tool Selection	<ul style="list-style-type: none"> <li>Data is masked and shared with Country A so that individuals cannot be identified</li> <li>A universal masking rule is applied for data transfer</li> </ul>
<b>Flow of Cross-Border Data Transfer and Tools Used</b> <p>For data management, use cloud server at each country for local management.</p> <div>           ① Europe → Country A: Share masked secondary data with Country A            ② Thailand, Country B, Country C → Country A: Share masked secondary data with Country A         </div>				Barriers/Needs in Tool Usage	<ul style="list-style-type: none"> <li>Created information masking rules with law firms / consulting firms at both entities in Country A / Europe, which cost tens of million yen.</li> <li>Local entities research legal aspects such as personal information protection regulations, while HQ in Country A takes the lead regarding data processing</li> <li>As for data usage, a Data Utilization Promotion Office was launched in FY2021, and a data utilization strategy is under consideration. Specific needs are expected to emerge in the future.</li> </ul>
				Comments on CBPR	(Not mentioned)



## 9 US Device Manufacturer

Since both internal / external cross-border data transfers are required, the company chose SCC customized in line with the regulations of each country

## Company/Business Overview

## Company overview

- Business type: Construction machinery manufacturer
- Size: Listed in NYSE

## Cross-Border Data Transfer Needs

## Customer data

- Name, address, TEL, ID no. (in some countries), financial status, etc.
- For vehicle sales/purchase and after-sale maintenance, marketing purpose

## Dealer info

- Employee information of dealers in each country
- For internal HR purpose

## Other marketing and industry info

- Data transaction bet JD and others in some cases

## Regulatory Compliance Method

### Selected Tool

- Uses GDPR-compliant SSC (US HQ - EU entity) for EU customer data
- For the data in other regions, concludes SSC with items edited to meet the regulations of each country based on SCC
- Concludes GDPR-compliant SSC for cross-border data transfer with vendors outside the Group

## Reasons/Process of Tool Selection

- HQ/each region has a specialized person called "privacy champion", and HQ selects a tool with the champion of each region
- Discusses response in comparison with the BM using a disclosed CISCO survey report in some cases
- As an operation, establishes a system to allow opt-in / opt-out
  - Applies opt-in; when the customer purchases a vehicle, presents the company's privacy notice, has customers tick to agree on "the usage for business execution" on each item, and stores only the items for which the consent is obtained on own server
  - All regions have privacy contacts and have a function to support demand for opt-out of customer data

## Barriers/Needs in Tool Usage

- It is practically difficult to define detailed data usage with SCC, and having to conclude SCC again for changes causes inconvenience
  - Data type (What), usage (How), purpose of the specifications (Why) must be clarified on SCC
  - Discussion was needed on what issues might arise in the future due to data use restrictions
  - in the era that API is actively used, it is time consuming to make sure that data not permitted by the SCC will not be used

## Comments on CBPR

(Not mentioned)

## Flow of Cross-Border Data Transfer and Tools Used

Provides local data servers for each region to manage data

- ① Europe → US: SCC + consent of individual customer
- ② Other (excl. China) → US: Localized SCC + consent of individual customer



## 10 Housing Product Manufacturer (as of 2014-2015)

To build a global HR system, the company chose to sign contracts with group companies and individual employee agreements on its own, since it was before the GDPR was launched

### Company/Business Overview

#### Business overview

- Business type: housing product manufacturer
- Holds Gr com in EU / US / China through M&A

### Cross-Border Data Transfer Needs

Data subject	Data type	Purpose of use
Employee (Managerial)	Name, age, gender, address, photo, background	To establish global common evaluation system for employees' career development

### Regulatory Compliance Method

#### Selected Tool

- Europe → Country A
- Parent company in Country A and subsidiary/sub-subsidiary in each country conclude consent on contents of data collection and usage
    - Developed own form as there was no SCC template for GDPR
  - In addition, parent company in Country A and employees conclude consent on contents of data collection and usage
- China / Country B / Country C, etc. → Country A
- The regulations in China was not as strict in 2014 thus handled employee information of subsidiary in China with the same method as EU
- Europe → Country A → US
- Adopt safe harbor when US employee manage EU employee

#### Reasons/Process of Tool Selection

- 3 internal + 3 external attorneys completed the first stage in 6 months
- 2 HR + 1 Legal in parent company and 1 from foreign-affiliated law firm in Country A formed a team to study personal information protection
  - In Aug 2014, consent from employees were found required in addition to contract between parent company/subsidiary in Country A, and the team had to acquire employee consent within 1 month
- Since new CLO (Chief Legal Officer) took office in Apr 2015 who directed tighter response, contents of employee consent were reviewed

#### Barriers/Needs in Tool Usage

- Not many companies in Country A handled the regulatory compliance of cross-border data transfer from overseas subsidiaries back then, and even law firms were not sure what level of support was required
- It was before the GDPR enactment, and most initiatives were only to reduce the risk of employee complaints. Companies were only making efforts only out of good intentions
- It took ~3 months to directly obtain consent from employees of subsidiaries / sub-subsidiaries
- government support to reduce burden on private companies is required
- Even if adequacy decision is obtained, man-hours are not reduced if SCC or BCR are required, and there will be no point of obtaining an adequacy decision
    - Practical support is needed including distribution of template for employee consent forms

#### Comments on CBPR

(Not mentioned)

### Flow of Cross-Border Data Transfer and Tools Used

- ① Europe / China / Country B / Country C, etc. → Country A:
- SCC equivalent contract between parent company in Country A and subsidiary/sub-subsidiary
  - Conclusion of consent between parent company in Country A and individual employees
- ② Europe → US: Safe harbor agreement



## 11 Consumer Research Firm

Due to the low risk of sanctions for cross-border transfers, the company opted to keep the data use agreement only between group companies

### Company/Business Overview

#### Com overview

- Business type: survey com
- Parent com in Country A
- Acquired a com in EU through M&A

### Cross-Border Data Transfer Needs

Data subject	Data type	Purpose of use
Employee	Name Address TEL Background, etc.	Introduction of global HR system
Survey respondent	— (Aggregate the data to transfer)	—

### Regulatory Compliance Method

#### Selected Tool

- ① U.K. / Country A / Country B → consolidate to a server in Singapore
  - Enables transfer of employee data as employees and the group conclude contract using the template of U.K. government
  - Uses similar consent forms for non-UK regions
- ② Server in Singapore → Country A
  - Obtains permission for data usage with above consent forms

#### Reasons/Process of Tool Selection

- No need to support compliance with data transfer regulations as the data collected from users such as survey result, etc. are anonymized before aggregation
- Cross-border data transfers are necessary for global personnel affairs, but the risk of sanctions is lower for employees than for civilians, and the resources required to deal with this issue are limited
- Chief privacy officer at HQ of EU subsidiary (U.K.) lead compliance with laws and regulations

#### Barriers/Needs in Tool Usage

- Cannot follow the regulations of each country due to a lack of resources for localizing data usage consent in non-UK countries
- BCR acquisition is desired for in-group data transfer, but the company cannot allocate resources to obtain BCR, so it is forced to patch up the consent forms
  - "Want to use a tool with a template that enables in-group transfer of employee information"

#### Comments on CBPR

(Not mentioned)

### Flow of Cross-Border Data Transfer and Tools Used

- ① U.K. / Country A / Country B, etc. → Singapore:  
Employee / com exchange consent forms for data usage and obtain permission for data collection
- ② Singapore → Country A:  
Obtain data usage permission in Country A using the above consent form



## 12 Network Device Manufacturer

Network security assurance is the most important management strategy. Therefore, the company chose BCR and CBPR for common data governance on a global basis

### Company/Business Overview

#### Company overview

- Business type: network device manufacturer

### Cross-Border Data Transfer Needs

Data subject	Data type	Purpose of use
Data subject of the data handled by client companies	Data handled by client company	<ul style="list-style-type: none"><li>• Network device</li><li>• Security service</li><li>• Cloud service</li></ul>

### Regulatory Compliance Method

#### Selected Tool

- Develops common global SDPA (Super Data Protection Agreement) that complies with laws in each country, and concludes data usage agreements with customer companies
- Uses BCR and CBPR as cross-border data transfer tools

#### Reasons/Process of Tool Selection

- Acquired BCR and CBPR as cross-border data transfer tools
- Has privacy data team in each country and over 400 attorneys
  - Dedicated in-house privacy policy team in each country to discuss regulations / requirements and to update company-wide privacy policies

#### Barriers/Needs in Tool Usage

- Survey is easier in EU countries as they are in a union, but Asian countries and the US have their own data protection regulations, requiring a large survey cost
- In the US, each state has its own regulation, placing a huge burden even on the US companies for strict compliance
- For rare cases, such as regulatory exceptions, internal decisions are made to accept the risk and not act

#### Comments on CBPR

- The CBPR is excellent in that it provides certification and a framework that allows governments to discuss data transfers of personal information
- However, even if the US has obtained CBPR, it is necessary to check each state's regulations one by one, so it would be a very useful tool if this issue can be resolved
- In addition, if the CBPR has the objective of facilitating data distribution in the context of European data sovereignty becoming the mainstream, it will play an even more important role

### Flow of Cross-Border Data Transfer and Tools Used

Data is localized, with customer and inquiry information stored in data centers in each country

- ① Europe ↔ Country A: BCR
- ② Japan, Country B, Country C, etc. ↔ Country A: CBPR



## 13 Internet Service Company

Although cross-border data transfers are the main focus within the group, the company is global and has many branches, so there is a risk that data governance will not be effective, so BCR was not chosen, and SCC was used

### Company/Business Overview

#### Company overview

- Gave comprehensive response on the support by several internet service companies together

### Cross-Border Data Transfer Needs

- ① Personalization purpose
  - Need user characteristics information to make better search results and ad display for users
- ② AI-learning purpose
  - Need a large amount of user data for AI learning as a basis of the above personalization
  - Names are not needed, and anonymized data is sufficient e.g. age range. As a standard practice, preserves profiles and blur details to allow segmentation

### Regulatory Compliance Method

#### Selected Tool

- Handles both internal / external cross-border transfer with SCC

#### Reasons/Process of Tool Selection

- BCR certainly facilitates cross-border data transfers within a group compared to SCC, but for a Big Tech company, BCR is impractical because it is difficult to achieve full governance for all branches and the risk of violating BCR is inevitable
  - BCR is difficult to use as they can be audited, so if full governance is not in place, the audit becomes a risk
  - However, in order to achieve a level of data handling that allows BCR to be obtained, In-house SCCs are prepared against BCR standards
- SCCs can be written in accordance with the regulatory level of each country through the use of appendices, making it possible and realistic for the SCC to be tailored to the actual situation of the company

#### Barriers/Needs in Tool Usage

- When crossing datasets, several SCCs are needed based on the type of data and the purpose of its use. A few thousands SCCs have already been created. A large handling cost is an issue.
- A longlist of risks defined by SCCs is too exhaustive and not realistic
  - "DTIA (risk assessment evaluation) is also time-consuming and requires clearer and minimum necessary checklist items"

#### Comments on CBPR

(Note: since they base on the experts' understanding, they may differ from the reality)

- Unlike SCCs (where multiple SCCs are concluded between Company A and B according to data type and purpose of use), the CBPR can comprehensively handle an increase in the number of target companies and uses, and if there are shortcomings in the data governance systems of Company A and B, a contract between the two companies should be sufficient
- CBPR's attempt to spread outside APAC is appreciated from the perspective of Middle Eastern/African companies
  - "We think it is better to work with South America, the US, and APAC to expand our business in the Middle East and Africa than to deal with the EU's strict regulations."
  - "Currently there are only six certification authorities, and it will take a long time to get certification. I think it would be good to make the certification tool stronger so that, for example, the Irish Certification Authority can be trusted to grant certification."

### Flow of Cross-Border Data Transfer and Tools Used

- Big Tech basically has data centers in each country, keeps the data collected within the country, and uses it for purpose ①
- On the other hand, since data can be replicated, the company also has a backup (anonymized) data center in the EU, which is used for the purpose of ② above

Europe ↔ Country A : SCC



## 14 Cloud Vendor

Given the need for cross-border transfer among the corporate in-house servers, it is important as the management strategy to gain the trust of companies using the service. Therefore, the company chose BCR for common data governance on a global basis

### Company/Business Overview

#### Company overview

- Business type: cloud vendor

### Cross-Border Data Transfer Needs

Data subject	Data type	Purpose of use
Data subject of the data handled by client company	Data handled by client company	Provide cloud service

### Regulatory Compliance Method

#### Selected Tool

- Prepares a common global DPA<sup>1</sup> (complying with the most stringent legal and regulatory standards in approximately 20 countries) and obtains BCR on the basis of the DPA's descriptions

#### Reasons/Process of Tool Selection

- Explored the possibility of DPA, since cloud service client with cross-border transfer needs can rely on cloud vendor's DPA for data handling
- Also obtained BCR as it is possible to gain the trust of cloud service clients
  - "Since it is a secure service, Chinese and Vietnamese companies that are obligated to store their data domestically also use our service and hold their data in our data centers outside of the country"
- Organization includes a legal team and an incident team
  - The company has its own in-house legal team dedicated to understanding and responding to cross-border transfer requirements, and has spent more than several billion yen in response to this issue
  - A global incident team is also in place to respond to incidents and share knowledge within the group

#### Barriers/Needs in Tool Usage

- "The cost of researching requirements in all the regions where client companies are located was a major hurdle, and being a large cloud vendor allowed the company to respond"

#### Comments on CBPR

(Not mentioned)

### Flow of Cross-Border Data Transfer and Tools Used

Data centers are located in about 20 countries each, and the company clearly shares with client companies which data is stored in which data center

Europe ⇄ Country A, Country B, Country C, etc. BCR

1.DPA=Data Processing Agreement



15 Major US IT Company

Network security assurance is the most important management strategy. Therefore, the company chose BCR and CBPR for common data governance on a global basis

Company/Business Overview

Company overview

- Business type: Sales of computer equipment and software for business use

Cross-Border Data Transfer Needs

Data subject	Data type	Purpose of use
Data subject of the data handled by client companies	Data handled by client company	<ul style="list-style-type: none"><li>• Computer equipment for business use</li><li>• SaaS</li><li>• Cloud service</li></ul>

Regulatory Compliance Method

Selected Tool	<ul style="list-style-type: none"><li>• Uses the "One Trust" information website template to comply with the privacy laws of each country</li><li>• Uses BCR and CBPR for cross-border data tools and for gaining clients' trust</li></ul>
Reasons/Process of Tool Selection	<ul style="list-style-type: none"><li>• Introduced CBPR as it can prove the processes and technology to ensure that the company complies with the frameworks and guidelines, which leads to client trust</li><li>• To comply with the privacy laws of other countries, the company conducts a privacy assessment, defines the contents and location of the data set, activities (what the company wants to do), processes (how to process), and assets (hardware/software), and use the necessary templates from "One Trust"</li></ul>
Barriers/Needs in Tool Usage	<ul style="list-style-type: none"><li>• CBPR itself is a framework and does not support national privacy laws or US state laws. Certification provides credibility, nothing more, nothing less</li><li>• Complying with CBPR requires annual financial and time costs, and the one-year renewal period only allows global companies with management strength to obtain the certification</li></ul>
Comments on CBPR	<ul style="list-style-type: none"><li>• In order to have more countries and companies adopt CBPR, it is necessary to expand its functions and increase its convenience. To do so, differences in personal information between countries should be identified, common areas should be redefined as common laws, and countries should be able to communicate more easily with each other</li></ul>

Flow of Cross-Border Data Transfer and Tools Used

① Europe↔Country A : BCR

② Japan, Country B, Country C, etc. ↔ Country A : CBPR



## 16 Internet Service Company

Network security assurance is the most important management strategy. Therefore, the company chose CBPR for global common data governance

### Company/Business Overview

#### Company overview

- Business type: internet service

### Cross-Border Data Transfer Needs

Data subject	Data type	Purpose of use
User data	Membership information for internet service	Linkage of membership information

### Regulatory Compliance Method

#### Selected Tool

- Uses CBPR

#### Reasons/Process of Tool Selection

- As global companies including Google and Amazon have obtained CBPR, the company obtained it to keep up with the certifications obtained by competitors
- It also serves as proof that the company holds privacy and security certifications at global standards, which allows users to register safely, thereby stimulating membership registration

#### Barriers/Needs in Tool Usage

- If CBPR encompasses requirements, and if there is a tool that can successfully overcome the personal protection regulations of different countries with a single certification, it will lead to streamlining the economic use of companies

#### Comments on CBPR

- Recognized each difficulty as SCC<CBPR<BCR. However, since we have no experience in obtaining them, we base our judgment on what we have heard and our personal experience
- It is difficult from the business side to understand a very complex regulatory tool, and communication itself is also difficult because each department has a different perspective. Therefore, we think it would be useful to have guidelines and use cases

### Flow of Cross-Border Data Transfer and Tools Used

Korea⇄Country A : CBPR  
※Other details are unknown



# Agenda

1. Position of This Project
2. Research related to Cross-Border Data Transfers
3. Research on the Actual Utilization by Businesses
- 4. Summary of Research Results



## Summary

Against the backdrop of regulations/tools proliferation, businesses decide which tool to use based on the purpose/scope of their data transfers and costs

### Regulations/ Data Transfer Tools

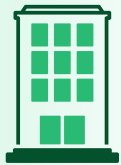


Most regulations allow cross-border personal data transfer if the situation meets specific requirements, but the requirements vary by regulations

- General requirements: consent of the data subject and a sufficient level of data protection in the transferee country
- In the countries that have GDPR-like regulations also approve:  
a legally binding instruments, certain certifications/seals, codes of conduct

Several countries (e.g., China, Russia, etc.) have data localization requirements in addition to cross-border data transfer regulations

### Business Operations/Needs



When there is a need for cross-border data transfers with companies outside the group, they are generally handled on a case-by-case basis. The most popular method is to use SCC

For data transfer among group companies, BCR is the most popular for businesses that aim to establish universal data governance. Using SCC is the standard if they don't aim to develop it.

CBPR is often used to gain credibility for the company's data governance




Businesses sometimes need to abandon data transfer to China due to its cost



## There is a need for a well-established forum with broad coverage that could gain external credibility

According to interviews from businesses, their main need is to meet minimum/appropriate level of protection requirements and gain credibility easily

From the perspective of this demand and the promotion of "reliable and free data distribution," there is a need for a new cross-border data transfer framework that satisfies the following:

Complies with regulations		Adequately protects data and complies with various regulations easily
Gains external credibility		Gains credibility from both authorities and external parties such as clients
Meets minimum requirements		Simple procedures/high predictability <ul style="list-style-type: none"><li>• Wide coverage (geographically, temporally, etc.)</li><li>• Clarified use cases, procedures, etc.</li></ul>

Future policy discussions will need to reflect on what kind of framework will be required to consider the above needs and the intent of the institutional design of regulations and tools in each country/region



# Needs and the Direction that the New Forum should take (Hypothesis)

Data Transfer Needs	Data Transfer Tools	Company
Transfer outside the group	Establish universal data governance	N/A (There is a need but no tool to address it)
	Comply with regulations on a case-by-case basis	<ul style="list-style-type: none"> <li>• Railway Company</li> <li>• Chinese Game Production</li> <li>• Equipment Manufacturer</li> <li>• Internet Service Company</li> </ul>
Transfer within the group	Establish universal data governance	<ul style="list-style-type: none"> <li>• Internet Service Company</li> <li>• Cloud Vender</li> <li>• Network Equipment Manufacturer</li> </ul>
	Comply with regulations on a case-by-case basis	<ul style="list-style-type: none"> <li>• Pharmaceutical Company</li> <li>• US Equipment Manufacturer</li> <li>• Residential Product Manufacturer</li> <li>• Internet Service Company</li> </ul>
		Establish internal rules for personal data management and voluntarily respond to risks without using existing tools
	Minimum Response (Low Risk)	<ul style="list-style-type: none"> <li>• Internet Service Company</li> <li>• Equipment Manufacturer</li> <li>• Apparel Manufacturer</li> <li>• Railway Company</li> <li>• Consumer Research Firm</li> </ul>
Common for both	Gain External Credibility	<ul style="list-style-type: none"> <li>• Network Equipment Manufacturer</li> <li>• Internet Service Company</li> <li>• IT Company</li> </ul>
Abandoned (The need for data transfer exists)	N/A	<ul style="list-style-type: none"> <li>• Apparel Manufacturer</li> <li>• Pharmaceutical Company</li> <li>• Equipment Manufacturer</li> <li>• Automotive Parts Manufacturer</li> </ul>

## Direction A

There is a need, but no tool is available to meet it

The new forum is going to fill this void.



## Direction B

Expand the effect of "credibility acquisition"

The new forum is going to comply with a wide range of regulations







[bcg.com](https://bcg.com)