APEC’s Cross Border Data Transfer Rules:
An Unfulfilled Potential, An Uncertain Future

June 2023

Jamael Jacob

Introduction

Many consider the unrestricted flow of data as driving today’s digital economy. For private enterprises, cross border data flows “improve productivity and reduce costs by enhancing scalability, improving supply chain efficiency, facilitating data analytics, and enabling digital collaboration”.¹ They are particularly crucial in laying the foundations for economies seeking long-term competitiveness.² Their impact, however, has a far greater reach. By spurring technological innovations and making more efficient data processing possible, they enhance almost every aspect of life, thereby benefiting just about everyone.

Throughout the years, the world has seen cross border data flows enjoy a steady growth. From 2005 to 2015, global data streams increased 45 times.³ Within that same time frame, the global GDP also saw an increase of over $2.8 trillion.⁴ An amount that is expected to reach around $11 trillion by 2025.⁵ In 2020, global data traffic hit 230 exabytes per month, with some predicting it to triple by 2026.⁶ This surge has coincided with the evolution of data flows in terms of complexity, volume, and nature, nurtured by a variety of interrelated factors, like the increased economic importance of data processing and a conducive internet architecture.⁷

All these developments have also come to highlight the downside to transnational transactions. Apart from implementation-related challenges, they also expose organizations and individuals to a variety of risks:⁸

- non-compliance with national laws
- unauthorized disclosure of personal data
- failure to uphold an individual’s data privacy rights, such as the right to access, correction, or erasure (of their personal data)
- inability to cooperate with regulators in connection with complaints
- regulators’ lack of capacity to investigate or enforce laws
- inability to guarantee the protection of personal data in countries with a low protection level
- conflicts between national and foreign laws
- possible access to data by foreign government
- overseas judicial decisions requiring the disclosure of data
- problems with recovery or secure disposal of data
- other harms, including loss of trust that results from the unlawful transfer and misuse of data

³ C & M International (n 1).
⁴ ibid.
⁵ ibid.
⁸ ibid.
To address or at least minimize these negative consequences, governments have adopted an array of regulatory mechanisms that may be classified into three categories: (1) open safeguards; (2) pre-authorized safeguards; and (3) limited transfers. The first is the most liberal in that it allows for some discretion in terms of how data transfers shall be secured, as long as prescribed guidelines are followed. The guidelines usually emanate from domestic statutes with extra-territorial application. In others, they consist of intergovernmental-level processes and multi-stakeholder participation across jurisdictions. The certification schemes envisioned under Article 42 of the European Union’s (EU’s) General Data Protection Regulation (GDPR), which encourages data controllers and data processors to voluntarily submit their data processing activities for assessment vis-a-vis the GDPR, are a prime example. Under the second model, government approval is typically required prior to data transfer, based on transparent criteria. China’s data export security assessment scheme is a case in point. The third is often characterized by strict and opaque requirements and a marked preference for data localization. Notable cases include regimes in Russia, Indonesia, and Vietnam.

The Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) Systems (collectively, “APEC Systems”) also represent the first type of regulation. They are certification systems which, although developed and maintained by governments of APEC economies, require private sector buy-in in order to work. More recently, a Global CBPR Forum (“Forum”) was also launched, but it is essentially an APEC Systems replica.

This report analyzes the APEC Systems and offers an assessment both in terms of its effectiveness (i.e., ability to deliver its promised benefits) and resilience (i.e., ability to overcome issues and survive). It checks on the implementation status of the participating jurisdictions after supplying a quick glance at other existing data transfer regimes as a necessary backdrop. A snapshot of the Forum is also provided, particularly since its ties to the APEC Systems inevitably shapes the latter’s long-term future. But with its implementation yet to commence, a more thorough assessment seems premature.

The aim is to provide essential information about today’s efforts to manage cross border data flows. The APEC Systems—and the Forum, to a lesser extent—occupy center stage. In addition to raising awareness, the Report hopes to facilitate more stakeholder engagements in future policy-making processes revolving around the protection of personal data as it travels from one corner of the world to the next.

Data protection and cross border transfers of personal data

Ensuring meaningful protection for personal data and related privacy rights while allowing for their free flow across jurisdictions stands at the crux of data protection regulations. However, just as there is a need to keep an organization’s internal data processing activities in check, so too is there a responsibility to police their public-facing operations, particularly those requiring the export of personal data.

Today, policies that address the risks posed by cross border data transfers may be classified into four types: (1) those seeking to prevent the circumvention of national privacy and data protection laws; (2) those guarding against data processing risks in other countries; (3) those asserting data protection and privacy rights abroad; and (4) those enhancing the confidence of consumers and individuals. They are not mutually exclusive, as most regulatory regimes tend to qualify under two or more of such categories. The APEC Systems can easily lay claim to all but the first.


10 Weber (n 7).
In order to arrive at a better appreciation of the APEC Systems, a survey of other notable data protection regimes and policy frameworks in force today is critical. They include the following:

OECD Guidelines

In 1980, the Organization for Economic Co-operation (OECD) adopted the Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (“1980 Guidelines”) to address concerns arising from the increased use of personal data and the risk to global economies resulting from restrictions to cross border data flows. The Guidelines have since been recognized as the first internationally agreed-upon set of privacy principles. They have influenced generations of related policies, including those of non-members. In 2013, they were updated to make them more responsive to changes in data use cases and new approaches in data protection. The aim, however, has remained constant: to promote and protect privacy, civil liberties, and the global free flow of information in order to foster the development of economic and social relations.

In the amended Guidelines, members are instructed not to impede cross border data transfers if they are to countries that: (1) substantially observe the Guidelines; or (2) have sufficient safeguards, including effective enforcement mechanisms and appropriate measures that ensure a continuing level of adequate protection consistent with the Guidelines. If there are to be any restrictions, they should be proportionate to the risks appreciated.

Convention 108+

In 1981, the Council of Europe developed the “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”. More popularly known as “Convention 108”, the treaty continues to be the only legally binding international instrument in data protection and welcomes member-signatories even among non-European countries.

At its core, Convention 108 requires parties to make sure their domestic laws apply its principles and ensure respect for the rights of individuals relative to the processing of their personal data. Its Additional Protocol of 2001 introduced additional requirements, such as the establishment of a data protection authority and the imposition of data export limitations. In 2018, an Amending Protocol was adopted to address more effectively the challenges brought by new information and communication technologies and to strengthen overall treaty implementation. It is now known as “Convention 108+”.

The Convention calls for the free flow of personal data between signatories. A party may only prohibit it if there is a real and serious risk that it would circumvent treaty provisions, or if such party is bound by harmonized rules of protection shared by States belonging to a regional international organization.

If the recipient is under the jurisdiction of an international organization or a country that is not a Party to the treaty, the transfer shall only be allowed if an appropriate level of protection is afforded either by: (1) the law of the country or international organization; or (2) standardized safeguards provided by legally binding and enforceable instruments between the entities involved in the transfer.

---

12 ibid.
13 Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data [2018] art. 14(1) <https://search.coe.int/cm/Pages/result_details.aspx?Objectid=09000016807c65bf> ibid art. 14(2) and 14(3).
Without such measures, the Convention still allows for data flows in certain instances: (1) the data subject has given consent; (2) the interests of the data subject require it; (3) there are prevailing legitimate interests provided by law and the transfer constitutes a necessary and proportionate measure in a democratic society; or (4) it constitutes a necessary and proportionate measure in a democratic society for freedom of expression.\textsuperscript{15}

\textit{General Data Protection Regulation}

While it is frequently perceived as the most exacting data protection law today, the EU’s GDPR was in fact designed to facilitate free-flowing data within the region, lowering related costs for the internal market. In force since 2018, it imposes obligations upon any organization in the world that targets or collects data related to EU citizens or residents. Harsh fines await violators, as demonstrated by data protection authorities that have regularly flexed their powers since the law’s effectiveness date.

For data transfers involving third countries (i.e., countries outside the European Economic Area, or EEA) and international organizations, the GDPR prescribes requirements that give transferred personal data the same level of protection it enjoys within the EEA. In general, it recognizes two ways through which EU-based organizations may engage in lawful cross border data transfers: (1) on the basis of an adequacy decision issued by the European Commission, or “EC”; or (2) where the EEA-based data controller or data processor provides appropriate safeguards, including enforceable rights and legal remedies for affected data subjects.\textsuperscript{16} “Appropriate safeguards” can be established by: (a) a legally binding and enforceable instrument between public authorities or bodies; (b) binding corporate rules (BCR); (c) standard data protection clauses adopted by either the EC or by a supervisory authority; (d) codes of conduct; or (e) certification mechanisms.

\begin{table}[h]
\centering
\begin{tabular}{|c|c|}
\hline
\textbf{GDPR-Sanctioned Certification Schemes} & \\
\hline
Under the GDPR, national and European authorities are encouraged to establish certification mechanisms that would demonstrate the compliance by data processing activities with the Regulation.\textsuperscript{17} Voluntary by nature, such mechanisms must indicate the presence of necessary safeguards.\textsuperscript{18} In addition, data controllers and data processors are also required to issue “binding and enforceable commitments” via contract or some other instrument that will apply said safeguards.\textsuperscript{19} That said, the responsibility of certified entities to comply with the GDPR is neither reduced nor minimized.\textsuperscript{20} \\
A certification is issued either by a certification body or the competent supervisory authority (i.e., data protection authority), based on a criteria approved by the latter or the European Data Protection Board (EDPB).\textsuperscript{21} If the criteria is EDPB-approved, a common certification is possible (i.e., the European Data Protection Seal).\textsuperscript{22} Each certification lasts for three years and \\
\hline
\end{tabular}
\end{table}

\textsuperscript{15} ibid art. 14(4).
\textsuperscript{16} According to most (if not all) data protection laws, “data controllers” refer to those entities that control the processing of personal data. “Data processors”, on the other hand, are entities that process personal data upon the instructions of a data controller, essentially performing such task on behalf of the latter.
\textsuperscript{17} Regulation 2016/679 General Data Protection Regulation [2018] OJ L119/1 art. 42.1
\textsuperscript{18} ibid., art. 42.2.
\textsuperscript{19} ibid.
\textsuperscript{20} ibid 42.4.
\textsuperscript{21} ibid 42.5.
\textsuperscript{22} ibid.
may be renewed.\textsuperscript{23} It may be withdrawn if the holder is no longer able to meet the certification criteria.\textsuperscript{24}

Certification bodies must be accredited either by the supervisory authority or a national accreditation body.\textsuperscript{25} Accreditation shall be for five years at most, but is renewable.\textsuperscript{26} It will be withdrawn if the holder is no longer able to meet the accreditation criteria, or violates the GDPR.\textsuperscript{27}

Apart from the GDPR, there are now two sets of Guidelines governing certification mechanisms. The first, Guidelines 1/2018, was formally adopted by the EDPB in 2019. It establishes broad requirements relevant to all types of certification mechanisms that will be developed under the Regulation. The second one, Guidelines 07/2022, was formally adopted on 14 February 2023.\textsuperscript{28} It discusses certification specifically as a transfer tool to third countries or international organizations. It establishes a two-step test and describes how the certification mechanism can be utilized by data exporters. It also discusses the different aspects of the certification mechanism: (1) purpose and scope; (2) actors involved; (3) accreditation requirements for certification bodies; (4) certification criteria; and (5) binding and enforceable commitments that need to be implemented.

Guidelines 07/2022 states that data exporters may rely on certification as a cross border data transfer tool; one that proves the existence of appropriate safeguards in the entity based on a third country.\textsuperscript{29} It is critical, though, that there be a legally binding document between the certification body and data importer requiring the latter to apply the certification criteria to all transferred data.\textsuperscript{30} Certification, as a transfer tool, should also be referred to in the principal contract between the transacting parties.\textsuperscript{31}

Other matters discussed by Guidelines 07/2022 include: (1) practical aspects of the certification criteria; (2) additional safeguards on the part of the data exporter; (3) situations when national law prevents compliance with commitments taken as part of certification; (4) implementation of binding and enforceable commitments; and (5) examples of supplementary measures that data importers may implement if the scope of the certification either includes or does not include the transit of data.

No official timeframe has been given for the implementation of GDPR-recognized certification systems.

Outside the two authorized routes, a number of derogations are also allowed but are expected to be invoked sparingly. Data transfers to third countries may still be possible if: (1) the data subject has given explicit consent; (2) the data subject enters—or is preparing to enter—into a contractual relationship where the transfer of data abroad is necessary; (3) it is necessary to conclude a contract

\textsuperscript{23} ibid 42.7.
\textsuperscript{24} ibid.
\textsuperscript{25} ibid 43.1
\textsuperscript{26} ibid 43.4.
\textsuperscript{27} ibid 43.7.
\textsuperscript{28} Guidelines 07/2022 on certification as a tool for transfers version 2.0 [2023] <https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_en_0.pdf>
\textsuperscript{29} ibid para 5.
\textsuperscript{30} ibid para 47.
\textsuperscript{31} ibid para 52.
between a data controller and a third party in the interests of the data subject; (4) it is for important reasons of public interest; (5) it is necessary to establish, exercise, or defend legal claims; (6) it is necessary to protect the vital interests of the data subject; and (7) it concerns the transfer of data from public registers. These grounds are a last resort for lawful transfers, typically reserved for exceptional cases and not for bulk or repetitive transfers.

**ASEAN Model Contractual Clauses**

In 2016, member-states of the Association of Southeast Asian Nations (ASEAN) introduced the Framework on Personal Data Protection as a means to strengthen data protection in the region and facilitate cooperation. The latter, in turn, is expected to boost regional and global trade, including the free flow of information. However, as is typical of ASEAN instruments, the regime does not create binding obligations. The most it offers is a modest glimpse into the countries’ views on cross border data transfers.

It states that, prior to any such transfer, an organization must first obtain the consent of data subjects or take reasonable steps to ensure that recipients will protect the personal data in a manner that is consistent with the other Framework principles. To facilitate the second option, the ASEAN Model Contractual Clauses for Cross Border Data Flows (MCCs) were brought in.

Officially endorsed in 2021, the MCCs are terms and conditions that may be included in binding contracts between parties engaged in cross border data transfers. They come in two modules, representing the two more common transfer scenarios: data controller-to-data processor and data controller-to-data controller. Designed for voluntary use by the private sector for inter-ASEAN data flows, the MCCs may also be utilized for intra-country transfers and transactions with parties based in non-member countries.

Parties are also given the option to adopt other transfer mechanisms recognized within the ASEAN, such as self-assessment, consent, codes of conduct, binding corporate rules, and certifications such as those facilitated by the APEC Systems.

**China’s Cross Border Data Transfer Requirements**

The Personal Information Protection Law (PIPL) of China took effect in 2021, and provides any entity intending to export personal data to a foreign recipient three routes to consider: (1) sign a standard contract formulated by the Cyberspace Administration of China (CAC); (2) undergo a government security assessment; or (3) obtain personal information protection certification conducted by a professional institution.

1. **Standard Contract Measures for the Export of Personal Information.** On 22 February 2023, the CAC released the final version of the Standard Contract Measures (SCM), which then came into effect.

---

32 ibid art. 49.
33 ibid art. 49(1).
36 ibid.
37 ibid.
force on 1 June 2023. As an option, this path is available only when all of the following conditions are satisfied: (a) the data controller is not a critical information infrastructure operator; (b) the volume of personal data involved does not exceed one million individuals; (c) the cumulative number of individuals whose personal data has been transferred overseas since January 1 of the previous year has not reached 100,000; and (d) the cumulative number of individuals whose sensitive personal information has been transferred overseas since January 1 of the previous year has not reached 10,000. Although prior approval is not required, a data controller needs to file its signed standard contract with the local CAC office within ten working days after the agreement’s effectivity date.

2. **Security Assessment of Overseas Data Transfer.** This route’s guidance was released on 7 July 2022 and took effect on 1 September 2022. In general, organizations go down this path if they: (a) transfer important data overseas; (b) are designated as a critical information infrastructure operators; (c) may process overseas the personal data of more than one million individuals, or sensitive personal information of at least 10,000 individuals, from the previous year; or (d) are required by the CAC to conduct security assessment based on other relevant laws or regulations. Under this system, they are required to conduct a self-assessment of their outbound data transfer, before applying for a security assessment that will be carried out by the CAC.

3. **Security Certification of Cross Border Processing of Personal Information.** This method facilitates the certification of data processing activities that involve certain cross border data transfers. The latest Guidelines were issued on 18 November 2022. On 16 March 2023, the Information security technology-certification requirements for cross border transmission of personal information (GB/T 35273) was re-released and were opened for comments until 15 May 2023. The latter provides a basis for certifying those involved in cross border data transfers. Organizations that process less than 10,000 sensitive personal information and/or less than 100,000 general personal information may obtain a certification for the following cross border data transfers: (a) those carried out among subsidiaries or affiliated companies of the same economic or business entity; and (b) those subject to the PIPL’s extraterritorial reach. Despite some notable differences, some observe that this certification scheme is comparable to the BCR System under the GDPR.

Whichever path a data exporter ends up taking, an indispensable precondition is a personal information protection impact assessment (PIPIA), which is akin to the EU’s data protection impact assessment. The need to engage with the CAC also appears inevitable, as is giving priority consideration to national security during assessments.

---

41 Measures for Data Export Security Assessment 2022 (CN) <http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm>
APEC Cross Border Privacy Rules System and the Privacy Recognition for Processor System

The APEC Systems operate under the APEC Privacy Framework, which is a set of principles and implementation guidelines meant to establish effective data protection measures that avoid barriers to information flows. They are supposed to ensure continued trade and economic growth among member-economies. Completed in 2005, the Framework was later updated in 2015. Its principles resemble those in the OECD Guidelines and overlap with many of those in the GDPR.

The Framework expressly calls for the development of a system of voluntary cross border privacy rules for the region. Such directive eventually translated into the CBPR System, and later, the PRP System.

CBPR System

In 2007, the APEC Ministers endorsed the “Data Privacy Pathfinder” proposal, a set of nine cooperative projects among participating APEC economies whose purpose is to develop a simple and transparent mechanism business enterprises can use to protect personal data moving across APEC economies. The projects ultimately set out to develop the CBPR System and came up with the following core documents:

1. a self-assessment questionnaire applicant organizations must accomplish
2. a set of program requirements Accountability Agents use to evaluate an applicant organization
3. a recognition criteria APEC Economies use when evaluating a prospective Accountability Agent
4. Cross Border Privacy Enforcement Arrangement (CPEA)
5. Charter of the CBPR Joint Oversight Panel (JOP)

The CPEA is a framework that facilitates effective cross border cooperation and voluntary information sharing between Privacy Enforcement Authorities (PEAs). It also makes sure that an economy has a law that implements the APEC Privacy Framework. Before an economy can join the CBPR System, the participation of its PEA in the CPEA is necessary. In most jurisdictions, a PEA is known as the data protection authority. The public body responsible for enforcing the data protection law, and which has the power to conduct investigations and pursue enforcement actions against erring entities.

The JOP, on the other hand, is a body composed of representatives from three participating economies, operating on behalf of the APEC Data Privacy Subgroup. It exercises oversight over the CBPR System, with the following core functions: (a) the issuance of reports about how an economy seeking to participate in the System has met the prescribed conditions; (b) making recommendations whether to recognize an organization as an Accountability Agent; and (c) considering the possible suspension of such recognition.

Elements

The System was finalized in 2011 and may be broken down into four distinct elements:

---

47 ibid 7.2(i).
48 ibid 7.2(ii).
49 ibid 7.2(iii).
1. **Self-assessment.** Using an APEC-recognized questionnaire provided by the Accountability Agent, an applicant organization assesses its own data protection policies and practices vis-à-vis the System’s program requirements. It must meet said requirements to hurdle the evaluation. In the questionnaire, the organization determines the scope of the certification it wishes to obtain by indicating key details, such as the types of personal data that will be covered and, if applicable, the list subsidiaries and/or affiliates governed by its data protection policies. Once accomplished, the questionnaire is returned to the Accountability Agent.

2. **Compliance review.** After it receives a completed questionnaire, the Accountability Agent conducts its own confidential assessment. It may supplement the questionnaire with additional questions, seek clarifications, or request for documentation.

---

**Recognition of Accountability Agents**

A prospective Accountability Agent must meet a recognition criteria that calls for an evaluation of its proposed program requirements and overall operations (e.g., dispute resolution procedures, policies and procedures for the avoidance of conflicts and process issues, ongoing monitoring and compliance reviews, and enforcement mechanisms). It must commit to release anonymized case notes and complaint statistics and cooperate with other Accountability Agents, especially when handling complaints. It must also agree to respond to requests from relevant government authorities of participating economies regarding its CBPR-related work.

The PEA of an APEC economy can be an Accountability Agent. Said economy must make the nomination and confirm that the PEA is a CPEA participant. It must also explain how the PEA can enforce the System’s program requirements. Meanwhile, one economy can also choose to use an Accountability Agent already recognized by another.

In all cases, the JOP reviews the request for recognition and issues its recommendation to the participating economies. If no objections are raised by the time the set deadline lapses, the request is deemed approved by the Electronic Commerce Steering Group, which is the APEC committee responsible for the APEC Privacy Framework.

An Accountability Agent can develop and use its own program requirements and questionnaire, but this requires prior approval of the APEC economies. Its overall assessment process may also exceed the System’s program requirements, but cannot fall below them.

3. **Recognition.** If an organization is determined by the Accountability Agent as being compliant with the System’s program requirements, it will be certified and will have the relevant details

---


51 ibid.

52 ibid p. 9.
of its certification published in a publicly accessible directory hosted by an APEC website. At a minimum, the following information about a certified organization will be displayed:\textsuperscript{53}

- name
- website
- link to privacy policy
- contact information
- Accountability Agent that issued the certification
- relevant PEA
- scope of the certification
- original certification date
- expiration date of the current certification

The directory informs stakeholders that a listed organization is an active participant in the CBPR System, allowing them to direct their questions and complaints to the appropriate entities (i.e., organization, Accountability Agent, or PEA).

4. \textit{Dispute resolution and enforcement.} The System is enforced by Accountability Agents and PEAs. In fulfilling their roles, the former may rely on either law or contract, while the latter take enforcement actions sanctioned by domestic data protection laws and regulations. If there is an CBPR-related complaint or issue that cannot be resolved by a participating organization or the concerned Accountability Agent, the PEA is expected to step in, investigate, and take enforcement action.\textsuperscript{54} When multiple jurisdictions are involved, the CPEA comes into play.

The APEC Data Privacy Subgroup is responsible for the governance of the CBPR System. Since the body only meets twice a year, the System is governed in such a way that it is able to operate without the Subgroup’s continuous involvement.

In performing oversight functions over the System, the JOP is assisted by working groups, including those on certification and enforcement. It can establish additional working groups, if necessary.

\textit{Participation by APEC Economies}

An APEC economy that wants to participate in the CBPR System must satisfy several conditions:\textsuperscript{55}

- Submit a letter indicating its intention to participate and confirming that it has at least one PEA participating in the CPEA.
- Indicate its intention to make use of at least one Accountability Agent.
- Explain how the System’s program requirements may be enforced within its jurisdiction.
- The JOP has submitted a report explaining how it has met the first three conditions.

\begin{center}
\textbf{Directory of Participating Economies}
\end{center}

\textit{Australia.} Australia officially joined the System on 23 November 2018 when the JOP put forward its final findings report. The Office of the Australian Information Commissioner has

\textsuperscript{53} Ibid p. 5.
\textsuperscript{54} APEC CBPR Systems, p. 10.
\textsuperscript{55} APEC CBPR and PRP Charter (n 46).
been a member of the CPEA since 2010. The country has yet to identify an Accountability Agent.

*Canada*. On 15 April 2015, Canada announced that it had formally joined the System, making it the fourth APEC member-economy to do so. It submitted its Letter of Intent in August of the previous year. There, it confirmed that the Office of the Privacy Commissioner of Canada is a participant in the CPEA. To date, however, the country still has no Accountability Agent.

*Chinese Taipei (Taiwan)*. Chinese Taipei also joined the System on 23 November 2018. Unlike other participating economies, it does not have a lone government authority in charge of enforcing its data protection regime, as imposed by its Personal Information Protection Act. To facilitate its participation in the System, at least 15 related ministries or commissions are involved.\(^\text{56}\) In June 2021, the Institute for Information Industry (III) became the country’s Accountability Agent.\(^\text{57}\)

*Japan*. Japan applied to participate in the CBPR System in June 2013. In May the following year, it was announced that the country had been accepted into the System. On 25 February 2016, the Japan Institute for Promotion of Digital Economy and Community was officially recognized as an Accountability Agent. The Personal Information Protection Commission is the country’s PEA.

*Mexico*. Mexico was the second country to participate in the System when its application was approved on 16 January 2013. Its PEA on record is the Federal Institute for Access to Information and Data Protection of Mexico. It has no Accountability Agent on record.

*Philippines*. The Philippines submitted its notice of intent to participate on 19 August 2019. It was accepted on 9 March 2020. The country’s PEA is the National Privacy Commission (NPC). On 15 October 2021, Commission invited companies and organizations to apply and become an APEC-accredited Accountability Agent.\(^\text{58}\)

*Singapore*. Singapore became the sixth country to join the System on 20 February 2018. It currently has one Accountability Agent: Infocomm Media Development Authority (IMDA). In June 2020, the Personal Data Protection Commission, the country’s PEA, amended the Personal Data Protection Regulations in order to recognize both APEC Systems as one of the modes for cross border data transfer.\(^\text{59}\) A template contract clause was also developed for the use of Singaporean data exporters.


Republic of South Korea. The country’s application was approved on 12 June 2017, making it the fifth APEC participant-economy. Its designated PEA is the Personal Information Protection Commission. It lists the Korea Internet and Security Agency as sole Accountability Agent.

United States of America. The US Department of Commerce announced the participation of the country in the System on 26 June 2012, with the Federal Trade Commission functioning as PEA. 60 There are currently five recognized Accountability Agents: (1) TRUSTe; (2) BBB National Programs; (3) NCC Group Security Services, Inc.; (4) Schellman & Company, LLC; (5) HITRUST. The US does not have a federal data protection legislation in place.

An economy can withdraw its participation any time by giving a month’s (written) notice.61 Any recognized Accountability Agent in that economy, including all organizations it has certified, will also be forced to terminate their participation.62

Apart from voluntary withdrawal, participation may also be suspended or terminated by a consensus determination by the other participating economies that either of the following conditions has been meet:63

1. Revocation, repeal, or amendment of a domestic law and/or regulation that makes it possible for the economy to participate in the System
2. The economy’s PEA has stopped participating in the CPEA

Privacy Recognition of Processors System

Just like the APEC Privacy Framework it is based on, the CBPR System only applies to data controllers and therefore leaves a significant policy gap. Consequently, this led to calls from data controllers for another certification system, one that would help them identify data processors that are safe to contract with (i.e., those with adequate data protection measures). Data processors were on board with this demand. They, too, wanted a mechanism that allows them to demonstrate their ability to effectively implement the data protection requirements of data controllers. The confluence of these factors led to the birth of the PRP System.

Just like the CBPR System, the PRP System also imposes basic requirements which entities must meet in order to be certified. Only this time, such entities are operating as data processors.

As a complement to the CBPR System, it has two core documents:

1. a self-assessment questionnaire applicant organizations must accomplish
2. a recognition criteria used to evaluate an entity seeking to become a PRP Accountability Agent

61 APEC CBPR and PRP Charter (n 46), 5.1.
62 ibid 5.3.
63 ibid 6.
The APEC Data Privacy Subgroup is also responsible for the governance of the PRP System, with the JOP also providing oversight. Similarly, working groups assist the JOP in the performance of its core functions.

**Elements**

As a near-exact copy of the CBPR System, the PRP System is broken down into the same four elements:

1. **Self-Assessment.** It also calls for an applicant’s assessment of its own data protection policies and practices through the use of an APEC-recognized questionnaire. This will be provided by and submitted to the Accountability Agent.

2. **Compliance Review.** The Accountability Agent will evaluate an organization’s policies and practices against the PRP System’s program requirements. Its assessment process may exceed the PRP standard through the use of its own questionnaire and/or program requirements, but they too must be pre-approved by the APEC economies. As far as the recognition of PRP Accountability Agents is concerned, the terms and the evaluation criteria are essentially the same as those for CBPR Accountability Agents.

3. **Recognition.** An organization deemed compliant with the PRP program requirements will be certified and will have the relevant details of its certification published in the same APEC website that features the CBPR directory. Directory details mirror those required for CBPR-certified organizations.

4. **Enforcement.** Since the Framework’s principles do not apply to data processors, the PRP System does not directly implement the Framework. This, however, does nothing to change the allocation of responsibilities in a data controller-data processor relationship, whether it be under applicable domestic data protection laws, the Framework, or even the CBPR System. As such, data controllers remain responsible for the data processing activities that data processors carry out on their behalf. Enforcement action against their data processors will have to go through them. This is consistent with the data protection laws of some APEC economies where direct action against data processors is not possible.

Despite the PRP System’s inherent limitations, it has mechanisms that ensure the effective oversight of PRP-certified data processors:

a. direct PEA backstop enforcement of the data processor’s compliance with the PRP System’s program requirements
b. enforcement by contract between the Accountability Agent and the data processor
c. government oversight over an Accountability Agent, and enforcement by the APEC Data Privacy Subgroup via the JOP
d. other mechanisms that have the effect of enforcing privacy

---

65 ibid p. 5.
66 APEC PRP System, p. 4.
67 ibid p. 3.
68 ibid p. 4.
Participation by APEC economies

The process for participating in the PRP System is also fundamentally the same as that for the CBPR System. However, in case an economy decides to stop its participation, it is required to give three months’ notice, instead of just one.\(^6\) Once an economy discontinues its participation, the Accountability Agent operating in that jurisdiction also ceases to take part in the System, along with its certified organizations. This fact must be indicated in the contract between Accountability Agents and their certified organizations.

At present, only two economies are participating in the PRP System: US and Singapore.

An economy may terminate its participation in the PRP System via voluntary withdrawal.\(^7\) Through a consensus, the other participating economies may also suspend or terminate its participation on the following grounds:\(^8\)

- Revocation, repeal, or amendment of a domestic law and/or regulation that makes it possible for the APEC economy to participate in the System
- The economy’s PEA has stopped participating in the CPEA
- The economy’s oversight and enforcement mechanisms that allow for the effective oversight of processors recognized under the PRP are no longer available

---

Global CBPR Forum

The Forum was established on 21 April 2022 via the Global CBPR Declaration (“Declaration”). With the APEC Privacy Framework and OECD Guidelines serving as backbone,\(^9\) its goal is to promote interoperability and help bridge different regulatory approaches to data protection and privacy.\(^10\) It lists the following as its specific objectives:\(^11\)

- establishment of an international certification system based on the APEC Systems
- support for free information flow and effective data protection
- a forum for information exchange and cooperation on related matters
- periodic review of data protection and privacy standards of members to ensure alignment of program requirements with best practices
- promotion of interoperability with other data protection and privacy frameworks

The Forum’s core documents consist of the Declaration and the Global CBPR Framework (“Global Framework”). These two are complemented by subsequent Forum issuances starting with the Global CBPR Forum Terms of Reference, which was released this April 2023 along with the Framework.

---

\(^6\) ibid p. 7.
\(^7\) APEC CBPR and PRP Charter (n 46), 5.
\(^8\) ibid p. 6.
\(^11\) Global CBPR Forum <https://www.globalcbpr.org/>
The Forum revolves around eight privacy principles: (1) preventing harm; (2) notice; (3) collection limitation; (4) uses of personal information; (5) choice; (6) integrity of personal information; (7) security safeguards; and (8) access and correction. Because they are interrelated, they are supposed to be read as a whole rather than as separate concepts.

Unlike the APEC Privacy Framework which only applies to the APEC CBPR System, the Global Framework already informs the CBPR and PRP components of the Forum. It also offers more guidance to participants regarding both domestic and international implementation.

**Participation**

In terms of participation, the Forum recognizes two types of participants: Members and Associates. Members take part in the CBPR and PRP Systems and set the Forum’s policy and strategy. Associates, on the other hand, are still preparing for their potential participation as Members. Such status lasts for two years, during which time they are expected to initiate an application for Membership.

To become a Member, economies must: (1) concur with the principles and objectives of the Forum, and demonstrate the alignment of their legal system with the Framework; (2) have at least 1 PEA as a participant in the Global Cooperation Arrangement for Privacy Enforcement (CAPE); and (3) either make use of at least one Accountability Agent and explain how the Global CBPR and PRP Systems may be enforced in their jurisdiction, or, in the alternative, demonstrate that the two systems are recognized by their legal system as a valid data transfer mechanism.

Meanwhile, those seeking to become an Associate must: (1) support the principles and objectives of the Forum; (2) have laws and regulations that protect personal data; and (3) have at least one public body responsible for enforcing their data protection laws and regulations, including having the power to investigate and pursue enforcement proceedings.

During the Forum’s launch, nearly all economies currently participating in the APEC CBPR System threw their support behind the initiative, leaving Mexico as the lone holdout. In April 2023, the United Kingdom reportedly submitted its application to join the Forum as an Associate, making it the first new jurisdiction to do so since the creation of the Forum.

Specific details have yet to be issued regarding the participation of PEAs, Accountability Agents, and entities interested in getting certified under the Framework. However, as far as the Accountability Agents and certified companies participating in the APEC systems are concerned,

---

76 ibid Part III, p. 9.
77 ibid Part IV, sec. A, p. 21-25.
80 ibid Annex A – Admission of Members and Associates to the Global CBPR Forum, sec. 10.
81 Global CBPR Forum TOR Annex A (n 80) sec. 3.
82 ibid sec. 4.
Forum members are supposed to consult them regarding their formal transition into the Forum. They will be automatically recognized based on the same terms they are recognized under the APEC systems. Accountability Agents, in particular, will be provided at least 30 days’ notice. So far, no specific transition date has been identified.

**Structure and Governance**

In terms of organizational structure, the Forum has the Global Forum Assembly (GFA). It consists of its Members and is regarded as the initiative’s policy-making body. Among other things, it implements the GFA annual work program, establishes and dissolves Committees, and reviews and endorses recommendations by those same Committees. Decisions are made based on consultation and consensus.

For the moment, three Committees have been established: (1) Membership; (2) Communications and Stakeholder Engagement; (3) and the Accountability Agent Oversight and Engagement. The central role of the first is to review and make recommendations regarding applications, while promoting participation in the Forum. The second promotes and protects its brand and manages its documents and records database. The third engages Accountability Agents, both existing and those applying to be one. This includes providing oversight and managing any complaint filed against them. The frequency of Committee meetings is determined by their respective Chairs.

Associates can participate in GFA meetings unless one is designated as exclusive to Members only. Meanwhile, their participation in Committee meetings is determined by the Committee Chairs.

---

**The good, with the bad**

A dozen years have elapsed since the APEC CBPR System was finalized. For the PRP System, it has roughly been eight years. Proponents of both regimes like to point to a number of benefits they supposedly offer both to certified organizations and the governments of participating economies.

First, they note that, as certification mechanisms, the APEC Systems provide participants with tangible proof of organizational commitment to data protection. This gives third parties confidence in their data processing operations, which, in turn, nurtures trust. Governments approve of this since it inspires greater participation in both state-sanctioned and private transactions. Moreover, organizations that do get certified are able to demonstrate to PEAs their compliance with data protection standards. This, at the very least, suggests a proactive dedication towards data protection.

Participation in the Systems also paves the way for the development of a privacy program roadmap. This is because compliance with data protection policies requires a robust privacy program. Building one can

---

85 Global CBPR (n 74).  
86 ibid.  
87 Global CBPR Forum TOR (n 79) sec.3.1(i-ii).  
88 ibid sec. 3.1(iii).  
89 ibid sec. 7.1(i).  
90 Global CBPR Forum TOR (n 79) sec. 3.1(iv).  
91 ibid sec. 3.2(iii).
be a daunting task, especially among small enterprises that have very limited resources. When organizations go through the application process, they are given a roadmap around which they can later establish a complete privacy program. This can also be a boon for governments, since participating organizations are more likely to invest in privacy programs given the added incentive. With Accountability Agents functioning as additional enforcement agents, PEAs are also able to reallocate resources to other important functions.

Meanwhile, certified organizations expect to encounter fewer compliance burdens when engaged in data transfers across participating APEC economies due to the multilateral nature of the APEC Systems and the enterprise-level certification they afford. After all, under the APEC Systems, it is possible to transfer data from one jurisdiction to the another— including subsequent transfers— as long as all entities involved are certified. In contrast, the proposed GDPR certification system focuses solely on transfers from within the EEA to a third country. Further transfers are prohibited by default. The APEC Systems also allow applicants to be evaluated as organizations. This means they need not undergo separate certification procedures for their different data processing activities. The proposed GDPR certification scheme will zero in on specific data processing activities. On the whole then, the APEC Systems could mitigate the impact of a fragmented global data protection regime using a common set of standards. A compliant entity is somewhat assured that it will also be able to comply with the minimum regulatory requirements of the different participating economies.

Proponents also describe the APEC Systems as offering end-to-end protection. This, since, for them to work, all entities involved in data transfer need to be certified. While official documents appear to be vague on this matter, a 2021 OECD Toolkit confirms just as much. On paper, this setup offers a better assurance to affected individuals, compared to the EU model where it is only the third-country data importer that will obtain a certification. The data exporter is merely assumed to provide adequate data protection since it is a GDPR-covered entity. This said, it is worth noting that the EDPB has not completely ruled out the possibility that transfers by data exporters may also be certified.

Finally, the APEC Systems’ respect for domestic regimes and dispute resolution resolution mechanisms are also often brought up. Indeed, the APEC Systems concede that each participating economy must decide its own approach to data protection. Their focus is on principles and flexibility, as opposed to top-down regulation. Consequently, they are less disruptive to local regulatory environments since participation does not replace domestic data protection obligations. At the same time, the APEC Systems manage complaints and dispute resolution through a handful of enforcement mechanisms. Accountability Agents are required to have mechanisms for: (1) receiving and investigating complaints about certified organizations and for resolving disputes between complainants and said organizations insofar as they relate to non-compliance with the Agent’s program requirements; (2) cooperating with other Agents when necessary in resolving disputes; and (3) for imposing penalties, including the referral of complaints to the concerned PEA if violations of applicable law are likely involved. PEAs, for their part, are required to cooperate and consider requests for assistance, as well as referrals for investigation or enforcement. It is worth noting, though, that very little evidence is currently available as regards the effectiveness of the all these measures.

---

93 Guidelines 07/2022 (n 22) para 15-16.
94 ibid para 19.
95 ibid.
96 APEC CBPR Systems (n 50) para 44.
98 ibid.
99 ibid para 13(d).
Such accolades, however, have not existed in a vacuum. These past several years, they have shared the limelight with issues and challenges that have hounded the Systems since their respective inception dates. Some problems are inherent in their design or implementation, while others are external factors beyond the control of the concerned stakeholders.

At the top of the pile is the perception that the Systems offer inadequate data protection. The APEC Privacy Framework’s standards have long been the subject of criticisms for being exceptionally weak. As one analyst notes, they are “at best an approximation of what were regarded as acceptable information privacy principles in 1980 when the OECD Guidelines were adopted”.101 This is lamentable considering the upgrade the OECD Guidelines themselves went through in 2013. Unlike the EU Data Protection Directive, the Framework did not build on the OECD regime to add stronger security measures such as a limitation on data retention. Worse, some aspects, particularly its implementation requirements, are seen as inferior to any other international privacy instrument. The Framework neither requires from its signatories any particular means of implementation nor provides any mechanism to verify if they have even done so. With no explicit country obligation to implement its standards, resorting to the courts to question a country’s failure to implement is futile if not outright unavailable.

The low participation rate among APEC members is also hard to ignore. Since the establishment of the CBPR System in 2011, less than half of APEC’s total membership have signed on to participate. Whether this is due to regulatory incompatibility or a plain inability of the other members to comply with the program requirements remains to be seen. In any case, among the nine that have joined, only five have Accountability Agents. So far, the US is the only country with multiple accredited entities. The numbers are even worse for the PRP System where only two countries have joined since 2015. Other regional or intergovernmental arrangements do not face a similar dilemma in that all parties subscribe to the agreed set of rules or principles. While there is currently no available data that adequately explains the dismal state of the two systems’ implementation, the poor turnout evokes a negative perception among those entertaining the idea of signing up. In the long run, this would impact some attributed benefits like cost-effectiveness, which are only relevant if stakeholder participation is high.

The APEC Systems also take on the inherent limitations of APEC as an organization, and this translates to enforcement challenges. As an organization of States, the APEC distinguishes itself by not having a constitution. It only operates by consensus and takes on commitments on a voluntary basis. Thus, APEC agreements do not have any legal status, and are best seen as agreed sets of aspirations supported by mere commitments to cooperate. This is evident in the case of the APEC Systems. The JOP Charter explicitly emphasizes that it creates no binding obligations on participating economies.102 This makes it easy for participants to simply walk away from their commitments. Also, unlike the EU or even ASEAN, APEC is a non-treaty organization and only has a small full-time staff. For that reason, neither the two systems nor any of its other initiatives can impose onerous tasks, especially on the Secretariat. Any system that lacks the resources to enforce its rules is setting itself up for failure. This gives little comfort to affected individuals who may one day have to insist on enforcement action if a certified organization fails to fulfill its obligations. Their only realistic recourse may be to rely on Accountability Agents that have limited track records in enforcement and obscure grievance mechanisms in place.

Another consequence attributable to the Systems’ APEC roots is their having no significant positive influence on domestic data protection regimes, unlike the GDPR and its cross border transfer mechanisms. They are, after all, not directly applicable regulations. As noted earlier, supporters consider this a positive trait as it shows the Systems do not interfere in local affairs. Domestic regimes are allowed to take their course. This, however, goes both ways. It also means they will not be in a position to improve local regulatory environments. Jurisdictions that have weak regulations are neither compelled nor motivated to

102 APEC CBPR and PRP Charter (n 46) 1.1(i).
adjust (for the better). The US is a perfect case study. Despite it being the most active participant of the Systems, thus far, its attempts to pass a federal data protection legislation have all failed to date. Absent such law, the country’s relations with jurisdictions that have strict data protection policies have noticeably been strained. Accordingly, if the goal is to present a credible alternative to GDPR, the Systems are far from achieving that objective. They have little to no persuasive effect at the moment.

Also perceived as a weakness of the Systems is the limited participation and representation of civil society in its operations. Despite claims that they promote multistakeholder cooperation, it is no secret that discussions and negotiations around the Systems have mainly been between state representatives and the private sector. Civil society representatives such as Privacy International and the Electronic Privacy Information Centre did participate in some early meetings but only upon invitation by specific member economies. In any case, they did not have any real power to influence decision-making due to their mere observer status. This is unfortunate, since having such groups in crucial conversations tend to ensure privacy and data protection concerns are always raised and heard, for the benefit of the general public.

Ironically enough, there is also the issue of fragmentation. That there are essentially two identical certification systems operating under the influence of the APEC Privacy Framework points to this obvious issue. This setup translates to duplicate efforts on the part of participants, whether they be an APEC economy, a prospective Accountability Agent, or an organization seeking certification. The culprit is none other than the APEC Privacy Framework which underpins both Systems—albeit indirectly in the case of the PRP System. With the Framework dealing only with data controllers, creating a separate but related system became necessary. This issue is noticeably absent in other regimes such as the GDPR where all relevant distinctions are addressed (i.e., data exporters vs. data importers, data controllers vs. data processors). The redundancy that results contradicts, or at least dilutes, the harmonization effort the Framework and the Systems are meant to exude. It remains unclear why revising the Framework in such a way that it would accommodate data processors has not been considered to this day.

Cost is also a major concern, particularly for potential organization-participants. In Singapore, the application fee alone is currently around $400. This is on top of the assessment fee which is payable to any of the seven assessment bodies appointed by the Accountability Agent. The total assessment fee is determined by the size of the applicant organization and other related factors. In the US, one Accountability Agent puts the total certification cost between $15,000 to $40,000 “on average”. Neither one of these figures would appeal to most organizations harboring any thought of joining the Systems. It would not be a stretch to assume that many would prefer other data transfer mechanisms (e.g., obtaining an adequacy decision from the European Commission), which, as far they are concerned, cost nothing.

Lastly, there is the fact that the Systems are constantly competing with other legal regimes. The APEC Systems form part of a data protection framework that is still searching for its place in a world heavily influenced by European data protection policies. Unlike the GDPR, which is often regarded as the standard against which all other data protection laws are judged, the APEC Privacy Framework has long been the subject of criticisms for being ineffective, as standards go. If the Framework itself is unable to prove its long-term relevance, the APEC Systems may gradually be discarded by its current participants and ignored by the rest. Two other major developments make the road ahead less optimistic: (1) China’s recent decision to develop and enforce its own cross border privacy rules; and (2) the launch of the Global CBPR Forum. Between the two, the latter seems to pose the greater threat, since its very presence makes the APEC Systems redundant, if not obsolete.

105 ibid.
Into the unknown

If today’s trends are any indication, cross border data flows will continue to increase by leaps and bounds. Efforts to regulate them will also become more pronounced and nuanced. Collaboration between countries and international organizations will be crucial if an institutional mechanism that allows for interoperability and seamless data flows is to be achieved. Verily, as state and private actors find more uses for personal data, attendant risks will also scale up and prompt more data protection legislation. While many will try to find balance and avoid installing unnecessary friction, there will also be those favoring silos and data localization schemes which are antithetical to free-flowing data. Examples of both these approaches are already in force today.

The APEC Systems belong to the first camp. Given their current setup, particularly their voluntary nature, one can appreciate their appeal to technology platforms and other big businesses. At the same time, however, it is this very same quality that explains why they can expect little support from other sectors like small commercial enterprises, civil society groups who favor more rights-centric regimes, or governments that champion data localization or harsh data export restrictions. This inevitably puts them in an uphill battle in their quest for relevance and broader recognition.

For proponents that remain to this day, they must work on strengthening the Systems, beginning with a long-overdue revision of the APEC Privacy Framework and by doing away, in particular, with the unnecessary fragmentation. Once it acknowledges by default the two widely-recognized roles in data processing (i.e., data controllers and data processors), the Framework lays the groundwork for a unitary system that is simpler, more efficient, and less costly to manage. The Global CBPR Forum appears to have started with a similar initiative, but has stopped short of removing the CBPR-PRP distinction. Revisiting the existing enforcement processes of the Systems is also necessary and should call for more binding commitments from the participants. Both these efforts will go a long way towards making the Systems a more compelling option for interested parties.

Resilience and long-term success are much more elusive aspirations. The Systems will have to contend with the sizable influence of the GDPR, including the latter’s position on cross border data transfers. Modern data protection laws make plain how much headway the EU policy already has over other regimes. It will not be easy to catch up, let alone overcome such an advantage. There have been previous attempts to align the APEC Systems with the EU model, such as the 2014 effort that mapped the requirements of the EU BCR System alongside those of the APEC CBPR System. But that project was not aimed at achieving mutual recognition and could, at best, be used only as basis for double certification.\(^\text{107}\)

Dealing with newcomers like China’s cross border data transfer rules is also unavoidable. As things stand today, the APEC Systems are poised to become obsolete, with the Global CBPR Forum emerging as their natural successor. For current participants, this offers little comfort given the two regimes’ nearly identical qualities. Sans the introduction of significant improvements, the Forum will only replace a program whose potential has yet to be confirmed at the time of its demise. It inherits that uncertainty like everything else about the Systems it has already appropriated. To guarantee success or at least ensure lasting viability, stakeholders must work to make the Forum a better version of the APEC Systems, and not just an untested clone.

In the meantime, individuals whose personal data make up the precious resource both mechanisms are supposed to protect are placed at a disadvantage, at least compared to their peers in the EU or other jurisdictions with more established data transfer rules. It is them who stand to lose the most. In case their

information is compromised while being processed abroad, they will likely find access to adequate relief quite limited, or worse, non-existent. For business enterprises, it can be anything from an inconvenience to a risky proposition. Many of them would agree that if there is anything worse than regulatory fragmentation, it is regulatory limbo.