




BENEFITS OF THE
APEC Cross-Border Privacy Rules

Protecting Information. Driving Growth.
Enabling Innovation.

JANUARY 2019



“CBPR rules will become the foundation of a globally-accepted system that **enables data to be shared throughout different regions with strong and trustworthy privacy protections.**”

– Christina Peters, former Chief Privacy Officer, **IBM**

“The APEC privacy rules offer the promise of significant benefits to companies, consumers and privacy regulators[.] We hope that many more APEC economies will soon join and help realize the system’s potential as **a model for global interoperability among privacy regimes.**”

– Edith Ramirez, former Chairwoman, **United States Federal Trade Commission**

“APEC CBPR certification is an important way for Merck **to demonstrate to our customers, to patients and other stakeholders that we are committed to our privacy values** and to accountable privacy practices in every region of the world.”

– Hilary Wandall, former Chief Privacy Officer, **Merck & Co., Inc.**

CONTENTS

INTRODUCTION

The Need for International Transfer Mechanisms	2
The APEC CBPRs: An Overview	3
History	3
How the CBPR System Works	4
Benefits for Businesses & Organizations	5
Benefits for Governments	7
The Market Power of the “CBPR Economy”	9
Interoperability: One Size Need Not Fit All	10

HOW TO TAKE ACTION

For Businesses & Organizations	11
For Governments	11

Introduction

Data is not the new oil. While it may be the new currency of the modern economy, it knows no geography; its responsible use – properly safeguarded – multiplies, rather than depletes, its potential impact; and electronic bits and bytes, alone, generally have no intrinsic value. Rather, it is the *free flow of data* – its ability to transcend borders, along with the value that innovative companies from all over the world can apply to it – that is the lifeblood of the 21st-century global digital economy. The technologies that are driving growth and innovation by providing scalable, safe, and secure service delivery – including cloud computing, 5G, IoT, artificial intelligence, blockchain, and more – are all empowered by cross-border, international flows of data.

Just as fundamental to the digital transformation that is reshaping our world, however, is *trust*. Citizens must have the assurance that their personal information will be protected while online, and governments and business alike cannot harness the power that data brings without providing for appropriate privacy and security safeguards. A vibrant global debate has therefore arisen around how to ensure the appropriate level of privacy for personal information and create trust in the online ecosystem, while not stifling the innovation that is driving today's data-driven economy.

Fortunately, a balanced, flexible, pro-growth and pro-innovation model exists: **the APEC Cross-Border Privacy Rules** system. Developed by the 21 economies of the Asia-Pacific Economic Cooperation (APEC) forum, the CBPR system is a voluntary, enforceable, accountability-based certification that allows for the responsible transfer of personal data across borders and between participating economies. The CBPRs provide governments and organizations a ready-built, internationally-recognized framework to ensure adequate protection of personal information while enabling the secure flow of data—and thus providing the full benefits of today's global digital economy.



THE NEED FOR INTERNATIONAL TRANSFER MECHANISMS

Countries have responded to their citizens' calls and the global discussion around privacy by enacting a wealth of national laws aimed at protecting the personal data of those within their borders. Over 120 countries have passed legislation related to personal data protection, with a significant increase in new laws since 2010. Meanwhile, global data flows increased by 45 times from 2005 to 2015, accounting for an increase of over \$2.8 USD trillion to global GDP. The most recent measure of the volume of global data flows (from 2016) showed 400 terabits being transmitted per second—and this figure is expected to increase nine-fold by 2020. By 2025, global data flows could account for \$11 trillion of global GDP.

This exponential growth in data – and the acceleration in value and benefits it can provide to governments and citizens alike – shows no sign of slowing. This data represents the information, communication, transactions, and media transmitted across borders that are essential to the modern economy. Even in-country e-commerce platforms and online services rely on the international movement of data. For companies, cross-border data flows improve productivity and reduce costs by enhancing scalability, improving supply chain efficiency, facilitating data analytics, and enabling digital collaboration. More importantly, for individuals and consumers, the seamless flow of data empowers innovations that enhance every aspect of life, from health and safety to economic empowerment, education, and social exchange.

Attempts to erect walls or draw sovereign borders that limit the movement of data in the name of “security” often undermine that very goal – and most certainly can deprive citizens of the benefits and promise of the digital economy. Charting a regulatory course and adopting transfer mechanisms to promote data flows and incentivize data-driven investment can catalyze significant economic growth. At the same time, governments must continue to create trust in the digital economy by standing up privacy legislation and frameworks to ensure personal data is appropriately safeguarded. The key, then, lies in balancing these two important priorities.

The APEC Cross-Border Privacy Rules system provides a mechanism for governments and business stakeholders to safeguard the free flow of data while protecting the privacy rights of individuals. As the first set of privacy principles developed specifically for the Asia-Pacific and parts of Latin America, the CBPRs allow companies and regulators to match local privacy approaches to a cross-border, international system.

The APEC CBPRs: An Overview

The APEC Cross-Border Privacy Rules are a system that enables businesses to demonstrate compliance with a commonly understood set of privacy standards that apply across the APEC economies, thereby establishing a level of certainty and predictability for companies that move data across borders, and an assurance of security for the individuals providing that data. Because it does not supplant the privacy laws of individual economies, it enables governments to enact strong protections around the use and movement of their citizens' personal information.

HISTORY

The CBPR system is built upon the **APEC Privacy Framework**, a principles-based privacy standard that was endorsed by APEC's 21 "economies" in 2004 and updated in 2015. The Framework, which is consistent with and borrows from the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980, updated 2013), is intended to promote a consistent approach to privacy and personal information protection in the Asia-Pacific while ensuring the free flow of data to promote economic development and regional integration.

The APEC Privacy Framework features nine high-level information privacy principles. These principles largely resemble those found in the OECD Guidelines, and also overlap with many of the principles related to data processing found in the European Union's General Data Protection Regulation (GDPR).

> Principles of the APEC Privacy Framework

- Accountability
- Prevent harm
- Notice
- Choice
- Collection limitation
- Uses of personal information
- Integrity of personal information
- Security safeguards
- Access and correction

While other international frameworks enact restrictions on data transfers and can place an undue compliance burden on organizations in the name of privacy, the APEC principles are consistent with the forum's overarching mission of driving economic growth, strengthening cooperation among its members, and expanding prosperity and economic inclusion among citizens of the Asia-Pacific.

Unlike other international privacy regimes, the APEC Privacy Framework does not restrict the international transfer of data based upon domestic legal requirements in the receiving country. Instead, APEC endorsed the accountability principle, rather than limitations on transfers, as a reflection of APEC's economic and growth-oriented mission and as more consistent with modern business practices. CBPR-certified organizations are held accountable for their compliance with the system's requirements and for providing adequate safeguards for privacy and data protection.

Current Participants: There are currently eight participating APEC economies in the CBPR system (in chronological order of joining): the United States, Mexico, Japan, Canada, the Republic of Korea, Singapore, Australia and Chinese Taipei. As of January 2019, the Philippines has also publicly stated its intent to join the system, and momentum for the CBPRs continues to grow.

HOW THE CBPR SYSTEM WORKS

Adopted in 2011 and endorsed by the 21 APEC heads of state, the CBPR system allows participating business and other organizations operating within the member economies to develop their own internal business rules and policies consistent with the specific CBPR program requirements upon which the certification is based in order to secure cross-border data privacy.

Getting Started. Interested businesses and other organizations begin the CBPR application process by submitting a self-assessment questionnaire and supporting documentation to a recognized **Accountability Agent** in their jurisdiction. These are APEC-approved¹ third-party organizations that review organizations' privacy policies and practices, certify them as compliant with the CBPR system, and handle frontline dispute resolution between individuals and CBPR-certified businesses and organizations.

The Accountability Agent then undertakes a compliance review and works collaboratively with the applicant to evaluate and ensure those policies meet the requirements of the CBPR system. Once complete, the Accountability Agent may certify the organization as CBPR-compliant and the organization will be recognized on the official APEC CBPR website. All organizations must undergo annual recertification.

Protecting Personal Information. Individuals and consumers can trust that CBPR-certified organizations will handle their data responsibly – even if necessary to transfer it across borders to provide a service or business process – in accordance with the internationally-recognized principles of the APEC Privacy Framework. As required by the CBPR system, Accountability Agents examine the privacy policies and practices of participating companies and certify that they responsibly safeguard and protect user data.

Resolving Disputes and Ensuring Enforcement. The CBPR model of third-party verification – by the Accountability Agents – is a unique aspect of the system. Individuals have a clear point of contact to seek efficient, timely resolution of any disputes. This frontline dispute resolution and enforcement structure is more efficient and allows government authorities to focus on the highest-priority enforcement needs. The domestic authorities appointed by each APEC CBPR economy provide the enforcement backstop to take appropriate action, as needed.

VOLUNTARY	FLEXIBLE	ENFORCEABLE
<p>Reflecting APEC's consensus-driven approach, the CBPR system is a voluntary set of operational program requirements based on the APEC Privacy Framework, that enables organizations and businesses to show their compliance with international standards for privacy and data protection – and to improve their own data privacy programs.</p>	<p>The APEC Privacy Framework explicitly calls for “flexibility in implementation” of its principles. The CBPR system is designed to accommodate – rather than displace – the unique domestic privacy frameworks and legislative approaches of participating economies. Similarly, certified organizations are allowed flexibility to develop policies that meet their unique needs, so long as they demonstrate compliance with the CBPR program requirements.</p>	<p>To participate in the CBPR system, each economy must designate a public authority that is “responsible for enforcing privacy law and that has the powers to conduct investigations or pursue enforcement proceedings.” And each economy must join the APEC Cross-Border Privacy Enforcement Arrangement (CPEA), a collaborative, multilateral mechanism to promote cooperation and facilitate enforcement among their privacy enforcement authorities.</p>

For information on the CBPR system and how to get started, visit www.cbprs.gov

¹Organizations seeking to become Accountability Agents must be located in a CBPR-participating APEC economy and undergo a review process by the Joint Oversight Panel (JOP) of the APEC Data Privacy Subgroup, which oversees and administers the CBPR system. The recommendation of the JOP will then be sent to all APEC member economies for a consensus determination of the suitability of the Accountability Agent's application. The initial endorsement is limited to one year and then two years thereafter.

Benefits to Business and Organizations

In a rapidly digitizing global economy, companies are increasingly required to transmit business and customer data to multiple entities in foreign markets. An Australian hotel may serve customers worldwide by relying on a payment processor from Japan and back-end business processes in the Philippines and Indonesia, all while leveraging safe, efficient cloud data services from a data center in Singapore. The APEC CBPR system would allow each of these to rely on a single, cohesive set of privacy standards for their international data transfers, while demonstrating a high-standard commitment to privacy protection across multiple jurisdictions in the Asia Pacific and Latin America.

As a flexible, business-driven approach to data protection, the CBPR framework relies on companies to set internal rules and procedures that meet high-standard principles of data protection, with external verification by third-party Accountability Agents and subject to enforcement by domestic privacy regulators. But because companies have the best understanding of their own data-related operations and infrastructure, the CBPR system allows them the flexibility to determine how best to meet data protection standards, eliminating inefficient and unnecessary regulatory burdens and restrictions on data flows.

“...the APEC Privacy Certification helps protect the exchange of personal information across borders, which is vital to our business. As we continue to grow in different regions throughout the world, we want to continue to build trust with our users, address concerns about privacy and be transparent about our data privacy practices.”

– David Glaubke, Director of Corporate Communications, Lynda.com (now owned by Microsoft)

Promoting trust among customers by demonstrating an organizational commitment to privacy

Companies in all sectors rely on customer data more than ever to deliver innovative, personalized and more compelling services. As high-profile reports of data breaches have increased in recent years, customers are increasingly seeking assurance that businesses to which they entrust their data have adequate measures in place to protect it. Communicating privacy policies to customers can be challenging, as evidenced by the lengthy, legalistic privacy notices on websites that few people ever read.

CBPR certification can provide companies with an instantly recognizable symbol of organizational commitment to privacy and data stewardship. Coupled with a company’s meaningful efforts to enhance data protection, certification can create a foundation of trust and goodwill that will enhance a company’s brand value.

Providing businesses with a road map to privacy protection

Large technology companies that rely heavily on user data have already invested significant resources in building up robust privacy protection policies. However, for companies in other sectors where personal data protection



has only recently been a business issue, or for small- and medium-sized enterprises that lack resources to develop expansive privacy programs, the CBPR certification process can provide a much-needed road map. The process of applying for and obtaining CBPR certification can help any enterprise whose business involves the transfer of data establish a baseline level of privacy protection, compliance, and trust with partners and consumers across international markets.

■ **Demonstrating good faith compliance to enforcement authorities**

Just as CBPR certification shows consumers that a company is committed to protecting their personal information, it can also demonstrate that commitment to privacy regulators and enforcement authorities. CBPR's requirements ensure that certified companies are fully compliant with local data protection laws, thus demonstrating a proactive commitment to safeguard user privacy. Neutral, third-party Accountability Agents mandated by the CBPR framework serve as an additional check to ensure compliance with data privacy regimes.

Moreover, in worst-case scenarios where data breaches result in a privacy-related enforcement investigation, CBPR certification may be considered as evidence of a company's overall good faith commitment to data protection – which is particularly beneficial when authorities account for steps already taken by organizations to protect privacy when assessing possible remedies and determining, and potentially mitigating, potential sanctions.

■ **Lowering compliance burdens and reducing trade frictions**

Companies that are CBPR-certified can rely on a cohesive set of privacy standards to enable the responsible transfer of data between participating companies and foreign markets. By facilitating compliance with a significant portion of economies across the Asia-Pacific and the Americas, the CBPR system alleviates the costly and time-consuming need to navigate individual national privacy regimes. In studies commissioned by the APEC Secretariat, companies that have obtained CBPR certification report achieving faster and less costly compliance with privacy laws both in and outside of APEC. Furthermore, businesses that enter into transactions with companies in other markets can rely on CBPR certification to ensure that adequate data protection standards covering the transaction are in place on both sides.

■ **Enabling a flexible, accountability-based approach**

The free flow of data is a major driver of innovation and economic productivity in the 21st century. The CBPR system recognizes this and seeks to eliminate unnecessary burdens and restrictions on cross-border data flows. Because businesses are best placed to determine how to achieve privacy goals with minimal disruption given their unique circumstances, the CBPR system is driven first and foremost by companies' commitment to the CBPR principles, rather than by top-down regulation.

Benefits to SMEs

The APEC CBPR system is particularly helpful to SMEs, whether startups that intend to be global companies from Day One or existing companies seeking new global markets.

- Provides a roadmap to establish privacy policies & procedures
- Allows flexibility in designing policies that meet individual company needs, while still ensuring adequate privacy protection
- Helps align an organization's policies to a range of international privacy frameworks
- Lowers overall compliance burden

Benefits to Governments

In the digital age, citizens expect that their data will be safeguarded appropriately, both within their own economies and when it flows across borders. Growing public concern regarding data breaches and misuse of personal information have, in many cases, led governments to consider legal and regulatory measures covering the outsourcing of their citizens' data to other economies. In this environment, the CBPR system can build trust between regulators, businesses, and citizens. Personal information is protected, while governments can incentivize the investment, innovation, and unique services promised by the fourth industrial revolution.

Increasing privacy protections for citizens

By joining the CBPRs, governments adopt a mechanism that can help ensure their indigenous businesses establish a baseline standard of privacy protections when dealing with consumers' personal information. In addition, by encouraging broad adoption of the CBPRs, governments can increase public trust that personal data is being treated appropriately, even when it is exported.

Delivering a ready-built, internationally-recognized framework to bolster privacy enforcement

Effective enforcement of data privacy is a challenge for any government, requiring significant capacity and resources. That challenge will grow as more industries digitize and data is used more widely across the economy to deliver new products and services. By installing a system of baseline privacy standards and an accompanying model for cross-border enforcement, the CBPRs offer governments a ready and scalable model to bolster data protection while enabling enforcement authorities to focus resources more strategically to address privacy concerns. Accountability Agents serve as a first line of defense against privacy-related complaints and manage dispute resolution, and the Cross-Border Privacy Enforcement Arrangement (CPEA) facilitates collaboration among enforcement authorities.

Enhancing growth, investment and competitiveness

With data-intensive activities occupying an increasing share of the global economy, economies that position themselves as trusted stewards of data will have a competitive advantage in attracting investment from modern industries and in spurring home-grown innovation and business development. By joining the CBPR system and facilitating the certification of more organizations, governments can take an important step towards supporting growth and exports in their own data-driven industries of the future.



■ Respecting unique national approaches to privacy

There is no “one-size-fits-all” solution for privacy. Recognizing that each economy must decide its own approach based on its unique economic, political and legal approaches, traditions, cultural practices and other factors, the APEC Privacy Framework is designed to be principles-based and flexible rather than prescriptive. While setting out a general framework, they give economies and companies flexibility in determining how they will implement and enforce the program requirements associated with CBPR certification. Moreover, joining the CBPRs does not displace local laws, but complements them by creating a new certification opportunity for companies in each economy.

■ Promoting global trade flows

Modern trade agreements increasingly include measures to ensure digital interoperability among trading partners. In the recent U.S.-Mexico-Canada Agreement (USMCA), the parties expressly recognized the CBPR system as “a valid mechanism to facilitate cross-border information transfers while protecting personal information.” The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) mandates that its parties “should encourage the development of mechanisms to promote compatibility between these different regimes [to protect personal information].” Implementation of the CBPRs lays the groundwork for promoting interoperability with privacy standards in other regions of the world, and allows countries to meet the standard of 21st-century trade negotiations, thereby providing an opportunity for governments to promote trade even more widely.

■ Facilitating compliance and dispute resolution efforts

Privacy principles are effective only if business and organizations comply with them, but developing new compliance processes or procedures can be a costly endeavor. The CBPRs offer governments a fully functional certification system that can be quickly scaled up to support compliance by companies and organizations of all sizes and sectors, without the need to create new processes or procedures from the ground up.

Further, the Accountability Agent system means that recognized third parties, subject to appropriate domestic enforcement authorities, handle the frontline consumer complaints and dispute resolution, thereby freeing up government resources to focus scarce resources on the highest priority issues and enforcement actions.

“ In the era of big data, where data is a source of industrial competitiveness, developing effective procedures for international data transfers and appropriate protection of personal data is important. To this end, Japan will continue to strive for the popularization of the CBPR system to encourage companies and entities developing business overseas to make efforts for the protection of personal information transferred across national borders. ”

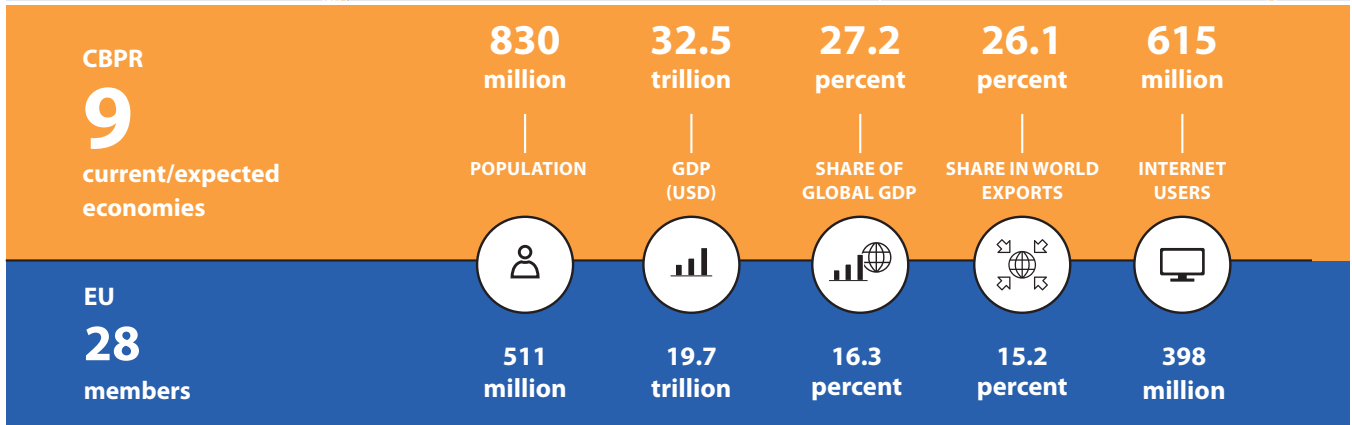
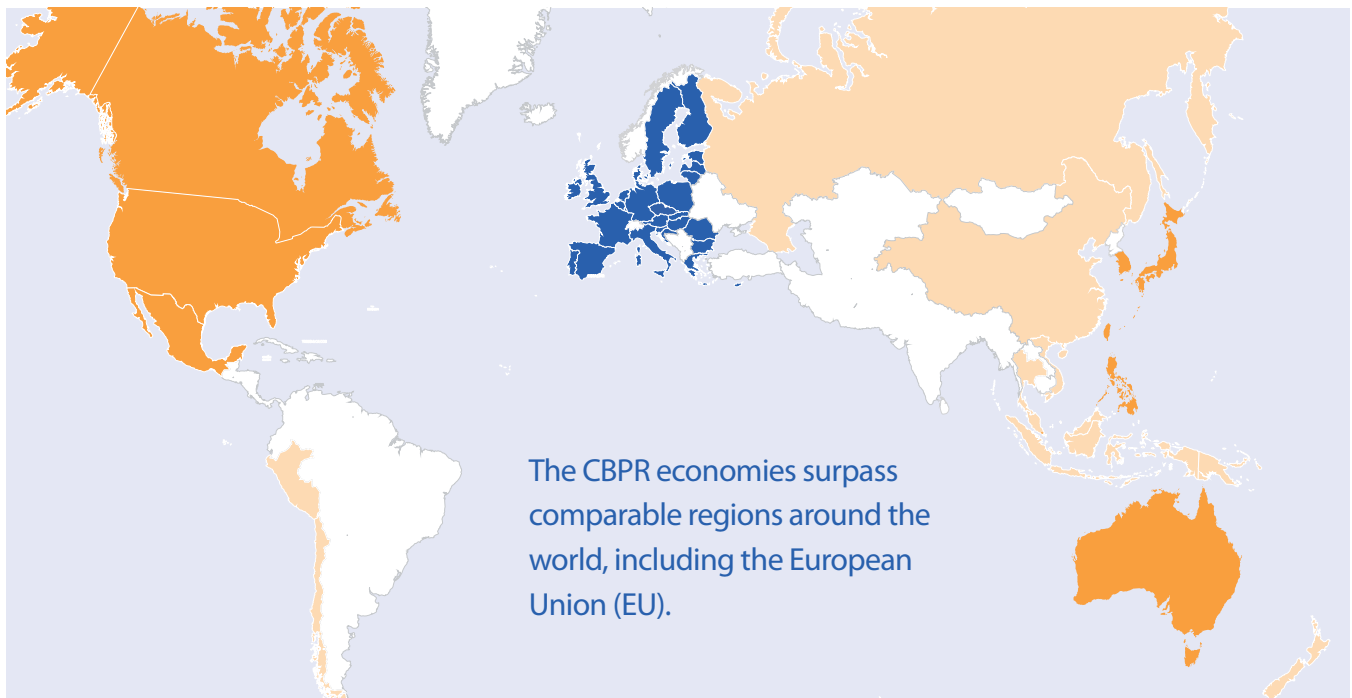
- Ministry of Economy, Trade and Industry, Japan

“ The seamless exchange of personal data [through the CBPR system] will enable certified Singapore businesses to plug into even more regional and global business opportunities. Meanwhile, our consumers will enjoy greater peace of mind when they shop or use vital services online. ”

- Personal Data Protection Commission, Singapore

Market Power of the “CBPR Economy”

The CBPR system covers the world’s largest and most dynamic marketplaces. By almost any economic or demographic measure, the CBPR region surpasses comparable areas around the world, including North America and the European Union (EU). Because of this considerable scale and scope, the CBPR system provides immense value for APEC economies and businesses by enabling them to facilitate data flows across the world’s largest single platform of its kind. By establishing a common framework for the Asia-Pacific, the CBPR system also creates an opportunity to promote interoperability with the EU and other regions and economies.



*The “CBPR Economy” = participating economies (U.S., Japan, Korea, Canada, Mexico, Singapore, Australia, Chinese Taipei) (as of January 2019) + announced intent to join (the Philippines).
The GDPR applies in the 28 EU member states and 3 additional states in the European Economic Area (Iceland, Liechtenstein, Norway).
Sources: IMF World Economic Outlook, WTO Trade Profiles and CIA World Factbook.

Interoperability: One Size Need Not Fit All

The acceleration in value and benefits that data-driven innovation is delivering in markets around the world will only increase in the years to come. To harness the true power of the digital revolution, society must promote mechanisms that enable global service providers and innovative new startups to reach citizens, while at the same time protecting personal information in order to maintain trust in the digital ecosystem. The key – and the challenge – is ensuring that one objective does not undo the other.

The APEC Cross-Border Privacy Rules are a flexible, adaptable model that responds to this challenge, while meeting the needs of the modern digital economy. There is no single “correct” way for ensuring privacy protections – rather, privacy frameworks can and should reflect the unique values of the cultures and citizens they seek to serve. Moreover, different models are needed for countries at different points on the spectrum between “developed” and “developing,” as well as those at different points of maturity in developing comprehensive privacy and data protection frameworks. **Flexible cross-border transfer mechanisms can provide the bridge between these varying national and regional frameworks, while ensuring consistent privacy safeguards.** Reflecting the diversity of APEC’s 21 different economies, the CPBRs were created to meet this important need.

Flexible, accountability-based approaches are also more conducive to modern business needs. Third-party verification, such as that overseen by CBPR Accountability Agents, can help ensure wider uptake by organizations, provide efficient dispute resolution between parties without draining government resources, and enable greater scalability of the overall system. And while bilateral agreements, “adequacy” determinations, and similar methodologies can provide certainty for those involved, the process is lengthy, complicated, and ultimately not practical for every market in the world. Models like the APEC CBPRs can transcend the differences in regional approaches, helping enable true global interoperability among privacy frameworks and creating a more seamless environment for the movement of data that underpins the benefits and innovation of the global digital economy.

As momentum continues to grow for the APEC CBPR system and its scope of coverage expands, it will stand as a model for global interoperability among privacy regimes.

How to Take Action

CHECKLIST FOR BUSINESS

Becoming CBPR certified offers a host of advantages to your business or organization. Below is a brief overview of the steps that you will take on your journey to becoming CBPR certified:

- ✓ **Determine Eligibility:** Does your economy participate in the CBPR system? If not, you will first have to work with your government and encourage them to go through the application process before businesses in that economy can become CBPR certified.
- ✓ **Identify an Accountability Agent:** To become certified you must be approved by a recognized Accountability Agent (AA). Determine if there is one in your economy that you can work with.
- ✓ **Complete a CBPR Intake Questionnaire:** This document (or a similar process offered by your Accountability Agent) is a comprehensive survey of your privacy policies that will be reviewed against the CBPR Program Requirements to determine if you are ready to become certified.
- ✓ **Work with your Accountability Agent:** While every Accountability Agent will operate somewhat differently, they will each have to engage in a collaborative process with you to verify compliance with the CBPRs and modify your policies and practices where necessary.
- ✓ **Ensure Compliance:** Businesses certified as CBPR compliant must attest annually to their compliance and continue to work with their Accountability Agents, to ensure compliance, for instance, following any material changes to privacy policies.

CHECKLIST FOR GOVERNMENTS

Adoption and implementation of the CBPRs provides APEC economies a ready-built framework to raise privacy protections, promote trade and investment, and showcase digital leadership within the region. Below is a brief overview of the steps to join and implement the CBPRs:

- ✓ **Join the APEC Cross-Border Privacy Enforcement Arrangement (CPEA):** Before joining the CBPRs economies must first make sure that at least one of their Privacy Enforcement Authorities participate in the CPEA, which creates a framework for cooperation that helps operationalize the CBPRs.

- ✓ **Submit an Application:** CBPR economies must submit a letter of intent to the Joint Oversight Panel that confirms their participation in the CPEA and intention to use at least one Accountability Agent. In addition, economies must provide a detailed overview of relevant domestic policies, authorities and enforcement practices, and complete the CBPR System Program Requirements Enforcement Map.
- ✓ **Engage in Consultation Process:** Economies that have submitted all of their documentation will then engage in a consultation process with the JOP Chair, which provides an opportunity to review the materials and request additional information.
- ✓ **Join the CBPR system:** Once the consultation is complete, the JOP will issue a findings report and determination as to whether the economy has met the requirements to join the CBPR system, under a simple majority. An economy will join the CBPR upon the issuance of a positive determination and JOP findings report.
- ✓ **Promote CBPR Adoption:** Joining the CBPR is only the first step towards adoption! Once an economy has joined, it is critical to establish an Accountability Agent (if not done so already) and begin to work with the business community to promote the awareness and benefits of CBPR certification.

For additional information and resources on
the APEC Cross-Border Privacy Rules,
visit the official website of the CBPR system:

www.cbprs.org

