THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

SIXTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

© 2019 Law Business Research Ltd

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

Sixth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2019
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

© 2019 Law Business Research Ltd

PUBLISHER
Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Joel Woods

SENIOR ACCOUNT MANAGERS
Pere Aspinall, Jack Bagnall

ACCOUNT MANAGERS
Olivia Budd, Katie Hodgetts, Reece Whelan

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Tommy Lawson

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anna Andreoli

SUBEDITOR
Charlotte Stretch

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC2A 4HL, UK
© 2019 Law Business Research Ltd
www.TheLawReviews.co.uk

No photocopying: copyright licences do not apply.
The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided was accurate as at September 2019, be advised that this is a developing area.
Enquiries concerning reproduction should be sent to Law Business Research, at the address above.
Enquiries concerning editorial content should be directed
to the Publisher – tom.barnes@lbresearch.com

ISBN 978-1-83862-062-2

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

© 2019 Law Business Research Ltd

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ALLENS

ANJIE LAW FIRM

ASTREA

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

BTS&PARTNERS

CLEMENS

KOBYLAŃSKA LEWOSZEWSKI MEDNIS SP. J.

MÁRQUEZ, BARRERA, CASTAÑEDA & RAMÍREZ

NNOVATION LLP

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VUKINA & PARTNERS LTD

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

© 2019 Law Business Research Ltd

CONTENTS

© 2019 Law Business Research Ltd

© 2019 Law Business Research Ltd

© 2019 Law Business Research Ltd

Chapter 3

APEC OVERVIEW

Ellyce R Cooper, Alan Charles Raul and Sheri Porath Rockwell[1]

I OVERVIEW

The Asia-Pacific Economic Cooperation (APEC) is a regional economic forum established in 1989 to enhance economic growth and prosperity in the region. It began with 12 Asia-Pacific economies as an informal ministerial-level dialogue group, and has grown to include the following 21 economies as of July 2019: Australia, Brunei, Canada, Chile, China, Hong Kong, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, Russia, Singapore, Taiwan, Thailand, the United States and Vietnam.[2] Because APEC is primarily concerned with trade and economic issues, the criterion for membership is being an economic entity rather than a nation. For this reason, its members are usually described as 'APEC member economies' or 'APEC economies.' Collectively, APEC's 21 member economies account for more than half of world real GDP in purchasing power parity and over 44 per cent of total world trade.[3]

The main aim of APEC is to fulfil the goals established in 1994 at the Economic Leaders Meeting in Bogor, Indonesia of free and open trade and investment in the Asia-Pacific area for both industrialised and developing economies. Towards that end, APEC established a framework of key areas of cooperation to facilitate achievement of these 'Bogor Goals'. These areas, also known as the three pillars of APEC, are the liberalisation of trade and investment, business facilitation, and economic and technical cooperation.

In 1999, in recognition of the exponential growth and transformative nature of electronic commerce, and its contribution to economic growth in the region, APEC established an Electronic Commerce Steering Group (ECSG), which began to work towards the development of consistent legal, regulatory and policy environments in the Asia-Pacific

1 Ellyce R Cooper and Alan Charles Raul are partners and Sheri Porath Rockwell is an associate at Sidley Austin LLP. The current authors wish to thank Catherine Valerio Barrad, who was the lead author for the original version of this chapter and made substantial contributions to prior updates. She was formerly a partner at Sidley and is now university counsel for San Diego State University.

2 The current list of APEC member economies can be found at www.apec.org/About-Us/About-APEC/Member-Economies.

3 See www.apec.org/FAQ.

© 2019 Law Business Research Ltd

area.[4] Soon thereafter, in 2003, APEC established the Data Privacy Subgroup under the ECSG to address privacy and other issues identified in the 1998 APEC Blueprint for Action on Economic Commerce.[5]

The work of the Data Privacy Subgroup led to the creation and implementation, in 2005, of the APEC Privacy Framework. Because of varied domestic privacy laws among the member economies (including economies at different stages of legislative recognition of privacy), APEC concluded that a regional agreement that creates a minimum privacy standard would be the optimal mechanism for facilitating the free flow of data among the member economies. While consistent with the original Organisation for Economic Co-operation and Development (OECD) Guidelines, the APEC Privacy Framework also provided assistance to member economies in developing data privacy approaches that would optimise the balance between privacy protection and cross-border data flows.

Unlike other privacy frameworks, APEC does not impose treaty obligation requirements on its member economies. Instead, the cooperative process among APEC economies relies on non-binding commitments, open dialogue and consensus. Member economies undertake commitments on a voluntary basis. Consistent with this approach, the APEC Privacy Framework is advisory only and thus has few legal requirements or constraints.

In 2011, APEC implemented the Cross-Border Privacy Rules (CBPR) system, under which companies trading within the member economies develop their own internal business rules consistent with the APEC privacy principles to secure cross-border data privacy. In 2015, APEC developed the Privacy Recognition for Processors (PRP) system, a corollary to the CBPR system for data processors. APEC is also working with the EU to study the potential interoperability of the APEC and the EU's new General Data Protection Regulation (GDPR), building upon the issuance in 2014 of a joint referential document mapping requirements of APEC and the EU's former data protection regime.

The APEC Privacy Framework, the CBPR and PRP systems, the cooperative privacy enforcement system and APEC–EU collaborative efforts are all described in more detail below.

II APEC PRIVACY FRAMEWORK

i Introduction

The APEC Privacy Framework, endorsed by APEC in 2005, was developed to promote a consistent approach to information privacy protection in the Asia-Pacific region as a means of ensuring the free flow of information in support of economic development. It was an outgrowth of the 1998 APEC Blueprint for Action on Electronic Commerce, which recognised that the APEC member economies needed to develop and implement legal and regulatory structures to build public confidence in the safety and security of electronic data flows (including consumers' personal data) to realise the potential of electronic commerce.

4 The ECSG was originally established as an APEC senior officials' special task force, but in 2007 was realigned to the Committee on Trade and Investment. This realignment underscores the focus within the ECSG, and its Data Privacy Subgroup, on trade and investment issues.

5 APEC endorsed the Blueprint in 1998 to 'develop and implement technologies and policies, which build trust and confidence in safe, secure and reliable communication, information and delivery systems, and which address issues including privacy'. See APEC Privacy Framework (2005), Paragraph 1 (available at https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)).

© 2019 Law Business Research Ltd

Thus, APEC's objective of protecting informational privacy arises in the context of promoting trade and investment, rather than primarily to protect basic human rights as in the European Union.

The APEC Privacy Framework represents a consensus among economies with different legal systems, cultures and values, and that at the time of endorsement were at different stages of adopting domestic privacy laws and regulations. Thus, the Framework provided a basis for the APEC member economies to acknowledge and implement basic principles of privacy protection, while still permitting variation among them. It further provides a common basis on which to address privacy issues in the context of economic growth and development, both among the member economies and between them and other trading entities. The Privacy Framework was updated in 2015 to account for the development of new technologies and developments in the marketplace and to ensure that the free flow of information and data across borders is balanced with effective data protections.[6] While updates were made to the preamble and commentary sections, the basic principles of the Framework remained unchanged. Further updates to the Privacy Framework are in the planning stages.[7]

ii The Privacy Framework

The Privacy Framework has four parts:

a Part I is a preamble that sets out the objectives of the principles-based Privacy Framework and discusses the basis on which consensus was reached;

b Part II describes the scope of the Privacy Framework and the extent of its coverage;

c Part III sets out the information privacy principles, including an explanatory commentary on them; and

d Part IV discusses the implementation of the Privacy Framework, including providing guidance to member economies on options for domestic implementation.

Objectives and scope of the Privacy Framework (Parts I and II)

The market-oriented approach to data protection is reflected in the objectives of the Privacy Framework, which include – in addition to the protection of information – the prevention of unnecessary barriers to information flows, the promotion of uniform approaches by multinational businesses to the collection and use of data, and the facilitation of domestic and international efforts to promote and enforce information privacy protections. The Privacy Framework was designed for broad-based acceptance across member economies by encouraging compatibility while still respecting the different cultural, social and economic requirements within the economies. As such, it sets an advisory minimum standard and permits member economies to adopt stronger, country-specific data protection laws.

The Privacy Framework cautions that the principles should be interpreted as a whole, rather than individually, because they are interconnected, particularly in how they balance privacy rights and the market-oriented public interest. These principles are not intended to impede governmental activities within the member economies that are authorised by law,

6 https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.

7 https://www.apec2018png.org/media/press-releases/revise-framework-conducive-for-e-commerce-environment.

© 2019 Law Business Research Ltd

and thus the principles allow exceptions that will be consistent with particular domestic circumstances.[8] The Framework specifically recognises that there 'should be flexibility in implementing these Principles'.[9]

The nine principles of the Privacy Framework (Part III)

Given that seven of the original APEC member economies were members of the OECD, it is not surprising that the original APEC Privacy Framework was based on the original OECD Guidelines. Similarly, the 2015 update was based on a 2013 update to the OECD's Guidelines.[10] The APEC privacy principles pertain to personal information about living individuals and do not apply to publicly available information or information an individual collects or uses in connection with their personal, family or household affairs. The principles apply to persons, businesses and organisations in the public and private sectors (referred to hereafter collectively as 'organisations') that control the collection, holding, processing or use of personal information. They do not apply directly to organisations that only act as agents or on behalf of others.

The APEC principles are based on the OECD Guidelines, but are not identical to them. Missing are the OECD Guidelines of 'purpose specification' and 'openness', although aspects of these can be found within the nine principles – for example, purpose limitations are incorporated in Principle IV regarding use of information. The APEC principles permit a broader scope of exceptions and are slightly stronger than the OECD Guidelines with respect to notice requirements. In general, the APEC principles reflect the goals of promoting economic development and respecting the different legal and social values held by member economies.

Principle I – preventing harm

This principle provides that privacy protections be designed to prevent harm to individuals from wrongful collection or misuse of their personal information and that remedies for infringement be proportionate to the likelihood and severity of harm.

Principle II – notice

The notice principle is designed to make sure that individuals know what information is collected about them and for what purpose it is being used. It requires that organisations take reasonably practicable steps to provide notice either before or at the time personal information is collected. Notice is not required for the collection or use of publicly available information.

Principle III – collection limitation

This principle limits the collection of personal information to only that which is relevant to the purpose of collection. It also stresses that, where appropriate, information should be collected with notice to, or consent of, the data subject.

8 See APEC Privacy Framework (2015), Paragraph 18.

9 See APEC Privacy Framework (2015), Paragraph 17.

10 See APEC Privacy Framework (2015), Paragraph 5.

© 2019 Law Business Research Ltd

Principle IV – uses of personal information

This principle limits the use of personal information to only those uses that fulfil the purpose of collection and other compatible or related purposes. If information is collected with the consent of the data subject, is necessary to provide a service or product requested by the data subject, or is required by law, limiting the use of information to the purposes for which it was originally collected does not apply.

Principle V – choice

The choice principle directs that, where appropriate, individuals be provided with mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information, with an exception for publicly available information. This principle also contemplates that, in some instances, consent can be implied or is not necessary.

Principle VI – integrity of personal information

This principle states that personal information should be accurate, complete and kept up to date to the extent necessary for the purpose of use.

Principle VII – security safeguards

This principle requires that security safeguards be applied to personal data that are appropriate and proportional to the likelihood and severity of threatened harm, the sensitivity of the data and the context in which it is held, and that the safeguards be periodically reassessed.

Principle VIII – access and correction

The access and correction principle provides that individuals have the right to access their personal information, which includes the right to obtain the information within a reasonable time of the request and in a form that is generally understandable. Individuals may also challenge the accuracy of their personal information and request appropriate correction. This principle includes exceptions when the burden of access or correction outweighs the risks to individual privacy, the information is subject to legal or security holds, or where the privacy rights of other individuals may be affected.

Principle IX – accountability

This principle requires that a data controller be accountable for complying with measures that give effect to the nine principles and that, when transferring personal information, it should take reasonable steps to ensure that recipients also protect the information in a manner that is consistent with the principles. This has often been described as the most important innovation in the APEC Privacy Framework and it has been influential in encouraging other privacy regulators to consider similar accountability processes tailored to the risks associated with specific data.

Unlike other international frameworks, the APEC Privacy Framework neither restricts the transfer of data to countries without APEC-compliant data protection laws nor requires such a transfer to countries with APEC-compliant laws. Instead, APEC adopted the accountability principle in lieu of data import and export limitations as being more consistent with modern business practices and the stated objectives of the Privacy Framework.

© 2019 Law Business Research Ltd

Implementation (Part IV)

Because APEC is a cooperative body, the member economies are not required to convert the Privacy Framework into domestic legislation. Rather, the Privacy Framework encourages the member economies to implement it without requiring or proposing any particular means of doing so. It suggests that there are 'several options for giving effect to the Framework [. . .] including legislative, administrative, industry self-regulatory or a combination of these policy instruments'.[11] The Framework advocates 'having a range of remedies commensurate with the extent of the actual or potential harm to individuals resulting from [] violations' and supports a choice of remedies appropriate to each member economy.[12] The Privacy Framework does not contemplate a central enforcement entity.

Thus, the APEC Privacy Framework contemplates variances in implementation across member economies. It encourages member economies to share information, surveys and research and to expand their use of cooperative arrangements (such as the Cross-Border Privacy Enforcement Arrangement (CPEA) (see Section III.iii)) to facilitate cross-border cooperation in investigation and enforcement.[13]

iii Data privacy individual action plans (IAPs)

Data privacy IAPs are periodic, national reports to APEC on each member economy's progress in adopting the Privacy Framework domestically. IAPs are the mechanism of accountability by member economies to each other for implementation of the APEC Privacy Framework.[14] The IAPs are periodically updated as the Privacy Framework is implemented within each such economy. As of 2019, 14 member economies have IAPs.[15]

II APEC CROSS-BORDER DATA TRANSFER

i Data Privacy Pathfinder initiative

When originally enacted in 2005, the APEC Privacy Framework did not explicitly address the issue of cross-border data transfer, but rather called for cooperative development of cross-border privacy rules.[16] In 2007, the APEC ministers endorsed the APEC Data Privacy Pathfinder initiative with the goal of achieving accountable cross-border flows of personal information within the Asia-Pacific region. The Data Privacy Pathfinder initiative contains general commitments leading to the development of an APEC CBPR system that would support accountable cross-border data flows consistent with the APEC Privacy Principles.

The main objectives of the Pathfinder initiative are to promote a conceptual framework of principles for the execution of cross-border privacy rules across APEC economies, to develop consultative processes among the stakeholders in APEC member economies for the development of implementing procedures and documents supporting cross-border privacy

11 See APEC Privacy Framework (2015), Paragraph 37.

12 See APEC Privacy Framework (2015), Paragraphs 53, 37.

13 See APEC Privacy Framework (2015), Paragraphs 57–64.

14 See APEC Privacy Framework (2015), Paragraph 55.

15 See https://www.apec.org/Groups/Committeee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.

16 See APEC Privacy Framework (2005), Paragraphs 46–48.

© 2019 Law Business Research Ltd

rules and to implement an accountable cross-border privacy system. Both the CBPR system and the CPEA – cross-border privacy systems that facilitate data protection and privacy enforcement – are outcomes of the Pathfinder initiative.[17]

ii The CBPR system

The APEC CBPR system, endorsed in 2011, is a voluntary accountability-based system governing electronic flows of private data among APEC economies. As of July 2019, eight APEC economies participate in the CBPR system – Canada, Japan, Mexico, South Korea, Singapore, the United States, and the two most recent additions, Australia and Taiwan – with more expected to join.[18] The CBPR system is designed to build consumer, business and regulator trust in the cross-border flow of electronic personal data in the Asia-Pacific region. One of its goals is to 'lift the overall standard of privacy protection throughout the [Asia-Pacific] region' through voluntary, enforceable standards set out within it.[19]

In general, the CBPR system requires organisations to adopt policies and procedures regarding the transfer of personal data across borders that meet or exceed the standards in the APEC Privacy Framework. Organisations that seek to participate in the CBPR system must have their privacy practices and policies evaluated by an APEC-recognised accountability agent to assess compliance with the programme. If the organisation is certified, its privacy practices and policies will then become subject to enforcement by an accountability agent or privacy enforcement authority.[20]

The CBPR system is governed by the Data Privacy Subgroup, which administers the programme through the Joint Oversight Panel, which is composed of nominated representatives of participating economies and any working groups the Panel establishes. The Joint Oversight Panel operates according to the Charter of the APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems Joint Oversight Panel and the Protocols of the APEC Cross-Border Privacy Rules System Joint Oversight Panel.[21] CBPR's website (cbprs.org) includes general information about the system, charters and protocols, lists of current participants and certified entities, submissions and findings reports and template forms.[22]

Member economies' participation in the CBPR system

Member economies must be certified to participate in the CBPR system before any private organisations subject to their jurisdiction can participate in the programme.[23] The CBPR certification requirements for APEC member economies are as follows:

a participation in the APEC CPEA with at least one privacy enforcement authority;

17 See Sections III.ii and III.iii.

18 http://cbprs.org/about-cbprs/.

19 See http://cbprs.org/government/.

20 A privacy enforcement authority is 'any public body that is responsible for enforcing Privacy Law, and that has powers to conduct investigations or pursue enforcement proceedings'. 'Privacy Law' is further defined as 'laws and regulations of an APEC Economy, the enforcement of which have the effect of protecting personal information consistent with the APEC Privacy Framework'. APEC Cross-Border Privacy Rules System, Policies, Rules and Guidelines, at 10.

21 See APEC Cross-Border Privacy Rules System Policies, Rules and Guidelines, at http://cbprs.org/documents/.

22 See www.cbprs.org.

23 http://cbprs.org/business.

© 2019 Law Business Research Ltd

b submission of a letter of intent to participate addressed to the chairs of the APEC ECSG, the Data Privacy Subgroup and the CBPR system Joint Oversight Panel providing:
- confirmation of CPEA participation;
- identification of the APEC CBPR system-recognised accountability agent that the economy intends to use;
- details regarding relevant domestic laws and regulations, enforcement entities and enforcement procedures; and
- submission of the APEC CBPR system programme requirements enforcement map.[24]

The Joint Oversight Panel of the CBPR issues a findings report that addresses whether the economy has met the requirements for becoming an APEC CBPR system participant. An applicant economy becomes a participant upon the date of a positive findings report.[25]

Accountability agents

The CBPR system uses third-party accountability agents to certify organisations as CBPR-compliant. Accountability agents can be either public or private entities and may also be a privacy enforcement authority. Under certain circumstances, an APEC economy may designate an accountability agent from another economy.

All accountability agents must be approved by the Electronic Commerce Steering Group or ECSG. The approval process begins with the submission by the proposed agent of an application and supporting documentation to the relevant authorities in the supporting economy in which the proposed agent intends to operate. The relevant authority will provide a preliminary review of the organisation and, if the authority supports the application, it will forward it to the chairs of the ECSG, the ECSG's Data Privacy Subgroup, and the Joint Oversight Panel. The Joint Oversight Panel then considers the application and will vote, by simple majority, on whether to recommend that the organisation be recognised as an accountability agent.

The proposed agent must meet the CBPR's requirements for accountability agents, which include:

a being subject to the jurisdiction of a privacy enforcement authority in an APEC economy participating in the CBPR system;

b satisfying the accountability agent recognition criteria;

c agreeing to use the CBPR intake questionnaire to evaluate applicant organisations (or otherwise demonstrate that propriety procedures meet the baseline requirements of the CBPR system); and

d completing and signing the signature and contact information form.[26]

Additionally, no accountability agent may have an actual or potential conflict of interest, nor may it provide any other services to entities it has certified or that have applied for certification.

Following an application and review process by the Joint Oversight Panel, the accountability agent can be approved by the ECSG upon recommendation by the Panel. Any

24 http://cbprs.org/government/economies-requirements/.

25 http://cbprs.org/government/economies-requirements/.

26 See http://cbprs.org/accountability-agents/cbprs-requirements.

© 2019 Law Business Research Ltd

APEC member economy may review the recommendation of any proposed accountability agent and present objections, if any, to the ECSG. Once an application has been approved by the ECSG, the accountability agent is deemed 'recognised' and may begin to certify businesses. Complaints about a recognised accountability agent are reviewed by the Joint Oversight Panel, which has the discretion to request investigative or enforcement assistance from the relevant privacy enforcement authority in the APEC economy where the agent is located.

Accountability agents are responsible for conducting initial certifications of organisations that want to participate in the CBPR system, and are also tasked with monitoring continued compliance with the APEC CBPR system standards. Towards that end, CBPR-certified organisations must submit annual attestations of compliance to their designated accountability agent. Accountability agents are responsible for ensuring that any non-compliance is remedied in a timely fashion and reported, if necessary, to relevant enforcement authorities. Accountability agents must publish their certification standards and promptly report all newly certified entities, as well as any suspended or terminated entities, to the relevant privacy enforcement authorities and the CBPR Secretariat.[27]

If only one accountability agent operates in an APEC economy and it ceases to function as an accountability agent for any reason, then the economy's participation in the CBPR system will be suspended and all certifications issued by that accountability agent for businesses will be terminated until the economy once again fulfils the requirements for participation and the organisations complete another certification process.

The CBPR system website contains a chart of recognised accountability agents, their contact information, date of recognition, approved APEC economies for certification purposes and links to relevant documents and programme requirements.[28] As of July 2019, the CBPR system recognises three accountability agents: TRUSTe, Schellman & Company, and the Japan Institute for Promotion of Digital Economy and Community.[29] TRUSTe and Schellman are recognised to certify organisations subject to the jurisdiction of the United States Federal Trade Commission (FTC). The Japan Institute for Promotion of Digital Economy and Community (JIPDEC) is recognised to certify organisations under the jurisdiction of the Ministry of Economy, Trade and Industry of the government of Japan. Accountability agents for other countries have yet to be designated.

CBPR system compliance certification for organisations

If an organisation is subject to the laws of an economy that is certified to participate in the CBPR system and an accountability agent has been approved for that economy, the organisation may apply to be certified to transfer personal information between APEC economies. The process of becoming certified begins with the submission of a self-assessment questionnaire and relevant documentation to an APEC-recognised accountability agent. The accountability agent will then evaluate the organisation and determine whether it meets the criteria for CBPR certification. Organisations that are certified are listed on the CBPR website. As of July 2019, 29 organisations have been CBPR certified, 26 of which are based

27 http://cbprs.org/accountability-agents/ongoing-requirements/.

28 See http://cbprs.org/documents/.

29 http://cbprs.org/accountability-agents/.

© 2019 Law Business Research Ltd

in the United States with the remainder based in Japan.[30] Certified companies must undergo annual recertification, which the accountability agent reviews. The number of certified organisations is limited by the fact that economies other than the United States and Japan do not have accountability agents to service organisations in their economies.

Effect of the CBPR on domestic laws and regulations

The CBPR system sets a minimum standard for privacy protection requirements and thus an APEC economy may need to make changes to its domestic laws, regulations and procedures to participate in the programme. With that exception, however, the CBPR system does not otherwise replace or modify any APEC economy's domestic laws and regulations. Indeed, if the APEC economy's domestic legal obligations exceed those of the CBPR system, then those laws will continue to apply to their full extent.

PRP system

Because the CBPR system (and the APEC Framework) applies only to data controllers, APEC member economies and data controllers encouraged the development of a mechanism to help identify qualified and accountable data processors. This led, in 2015, to the APEC PRP programme, a mechanism by which data processors can be certified by an accountability agent.[31] The PRP programme does not change the fact that data controllers are responsible for processors' practices, and there is no requirement that data controllers engage only PRP-recognised processors.[32] The PRP certification, which is conducted by approved PRP accountability agents, is designed to assure that processing is, at a minimum, consistent with the data processing requirements that data controllers are required to observe under CBPR rules.[33]

The Joint Oversight Panel of the CBPR administers the PRP programme pursuant to the Charter of the APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems Joint Oversight Panel and the Protocols of the APEC Joint Oversight Panel with Regard to the Privacy Recognition for Processors System.[34] The rules governing certification of economies and accountability agents closely track the CBPR framework, requiring the Joint Oversight Panel to engage in a similar evaluative process (e.g., issuing a findings report) as it does pursuant to CBPR rules.[35]

As of July 2019, two APEC economies have joined the PRP system – the United States and Singapore and the only two PRP-certified accountability agents are from the United States.[36] Seven processors have been certified under the programme, all of which are based in the United States.[37]

30 A current list of APEC-certified organisations can be found at http://cbprs.org/compliance-directory/cbpr-system.

31 The PRP Purpose and Background Document can be found at http://cbprs.org/documents/.

32 APEC Privacy Recognition for Processors ('PRP') Purpose and Background, found at http://cbprs.org/documents/.

33 APEC Privacy Recognition for Processors ('PRP') Purpose and Background, found at http://cbprs.org/documents/.

34 APEC Privacy Recognition for Processors ('PRP') Purpose and Background, found at http://cbprs.org/documents/.

35 https://www.apec.org/~/media/.../APEC%20PRP%20Rules%20and%20Guidelines.pdf.

36 http://cbprs.org/documents/.

37 http://cbprs.org/compliance-directory/prp/.

© 2019 Law Business Research Ltd

iii The Cross-border Privacy Enforcement Arrangement (CPEA)

One of the key goals of the Privacy Framework is to facilitate domestic and international efforts to promote and enforce information privacy protections. The Privacy Framework does not establish any central enforcement body, but instead encourages the cooperation of privacy enforcement authorities within the Asia-Pacific region. APEC established the CPEA as a multilateral arrangement to facilitate such interaction. The CPEA became the first mechanism in the Asia-Pacific region to promote cooperative assistance among privacy enforcement authorities.

Among other things, the CPEA promotes voluntary information sharing and enforcement by:

a facilitating information sharing among privacy enforcement authorities within APEC member economies;

b supporting effective cross-border cooperation between privacy enforcement authorities through enforcement matter referrals and parallel or joint enforcement actions; and

c encouraging cooperation and information sharing with enforcement authorities of non-APEC member economies.[38]

The CPEA was endorsed by the APEC ministers in 2009 and commenced in 2010 with five participating economies: Australia, China, Hong Kong China, New Zealand and the United States. Any privacy enforcement authority from any APEC member economy may participate and each economy may have more than one participating privacy enforcement authority. As of July 2019, CPEA participants included over two dozen Privacy Enforcement Authorities from 11 APEC economies.[39]

Under the CPEA, any privacy enforcement authority may seek assistance from a privacy enforcement authority in another APEC economy by making a request for assistance. The receiving privacy enforcement authority has the discretion to decide whether to provide such assistance.

Participation in the CPEA is a prerequisite to participation by an APEC economy in the CBPR system. As a result, each participating APEC economy must identify an appropriate regulatory authority to serve as the privacy enforcement authority in the CBPR system. That privacy enforcement authority must be ready to review and investigate a CBPR complaint if it cannot be resolved by the certified organisation or the relevant accountability agent, and take whatever enforcement action is necessary and appropriate. As more member economies join the CBPR system, this enforcement responsibility is likely to become more prominent.

III INTEROPERABILITY

Given the global nature of personal information flows, APEC's Data Privacy Subgroup has been involved in collaborative efforts with other international organisations with the goal of improving trust and confidence in the protection of personal information and, ultimately, to enable the associated benefits of electronic commerce to flourish across the APEC region. While privacy regimes such as the APEC Privacy Framework are drafted at

38 https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx.

39 https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx.

© 2019 Law Business Research Ltd

the level of principles, there are often very significant differences in the legal and policy implementation of those principles in different economies around the world. In an effort to bridge those differences and find commonality between the two largest privacy systems, in 2012 APEC endorsed participation in a working group to study the interoperability of the APEC and EU data privacy regimes. In August 2017, the APEC/EU Working Group met to discuss the impact GDPR will have on their undertaking.[40] These discussions followed the working group's 2014 release of a document (the Referential) that mapped the CBPR system requirements and rules under the EU's former data protection regime, the EU Data Protection Directive. The Referential identified common and divergent elements of both systems to help multinational companies develop global privacy compliance procedures that were compliant with both systems. In its August 2017 meeting, the Working Group agreed to work to develop a new joint work plan to update its previous work in light of GDPR, focusing on mechanisms that can be used to facilitate cross-border data flows and data protection enforcement between the APEC region and the EU.

In February 2019, the EU released an extensive study on data protection certification mechanisms, which included a comparative analysis of the certification criteria under GDPR and APEC's CBPR system.[41] The study found that the CBPR system was a 'good example' of how to set up certification oversight mechanisms, yet concluded that the CBPR's data transfer rules and redress mechanisms did not correspond to GDPR certification standards.[42] It remains to be seen if interoperability arrangements between the two systems can be developed.

IV THE YEAR IN REVIEW AND OUTLOOK

The APEC CBPR system saw some growth in 2018–2019. In late 2018, Australia and Taiwan joined the APEC CBPR system.[43] In early 2019, Schellman & Company was certified as a CBPR and PRP accountability agent for the United States, joining TRUSTe. Between June 2018 and July 2019, seven additional companies have become CBPR certified, including large companies with significant international presence, such as Mastercard and General Electric.[44] Seven US-based companies received PRP certifications during the same time period, including Box, Inc, Mastercard and General Electric.[45]

Significantly, in September 2018, the CBPR system was endorsed as a valid mechanism to facilitate cross-border information transfers between the United States, Canada and Mexico in the United States–Mexico–Canada Agreement, the new trade agreement that was drafted to replace NAFTA.[46] The parties to the agreement, which as of July 2019 is still awaiting ratification, agreed to 'cooperate and maintain a dialogue on the promotion and

40 https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Data-Privacy-Subgroup-Meeting-with-European-Union.

41 https://ec.europa.eu/info/sites/info/files/data_protection_certification_mechanisms_study_publish_0.pdf.

42 Id. at 5.

43 http://cbprs.org/news/.

44 http://cbprs.org/compliance-directory/cbpr-system/.

45 http://cbprs.org/compliance-directory/prp/.

46 https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19_Digital_Trade.pdf.

© 2019 Law Business Research Ltd

development of mechanisms, including the APEC Cross-Border Privacy Rules, that further global interoperability of privacy regimes.'[47] It is hoped that this endorsement of the CBPR will elevate the stature of the programme and encourage other economies to join.

In the United States, the FTC remains active in preserving the integrity of the CBPR system by targeting companies that falsely represent compliance with CBPR. The FTC brought its first such enforcement action in 2016, against Very Incognito Technologies Inc.[48] In 2017, the FTC reached settlements with three additional companies – Sentinel Labs, Inc, SpyChatter, Inc and Vir2us, Inc – in actions where the FTC alleged the companies had falsely represented that they participated in the APEC CBPR system.[49] In 2019, the FTC issued two warning letters against companies for making similar misrepresentations.[50]

The FTC has brought actions against other companies for similar misrepresentations in other trans-border programmes, such as the EU–US Privacy Shield programme.[51] The FTC's continued enforcement actions may signal that it intends to continue to play an active role in enforcement of cross-border data transfer certification programmes, including the CBPR.

47 https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19_Digital_Trade.pdf, at Art. 19.14(1)(b).

48 See In re Very Incognito Tech, Inc., FTC, No. 162 3034, final order, 21 June 2016.

49 www.ftc.gov/news-events/press-releases/2017/02/three-companies-settle-ftc-charges-they-deceived-consumers-about.

50 https://www.ftc.gov/news-events/press-releases/2019/06/ftc-takes-action-against-companies-falsely-claiming-compliance-eu.

51 In June 2019, the FTC approved a settlement with a company that falsely represented its compliance with the EU-US Privacy Shield programme, following its 2017 actions in approving settlements with three companies for similar misrepresentations. https://www.ftc.gov/system/files/documents/cases/182_3152_securtest_do.pdf; https://www.ftc.gov/news-events/press-releases/2017/11/ftc-gives-final-approval-settlements-companies-falsely-claimed.

© 2019 Law Business Research Ltd

Appendix 1

ABOUT THE AUTHORS

ELLYCE R COOPER

Sidley Austin LLP

Ellyce Cooper is a partner in the firm's Century City office and a member of the complex commercial litigation and privacy and cybersecurity practices. Ellyce has extensive experience in handling government enforcement matters and internal investigations as well as complex civil litigation. She assists companies facing significant investigations and assesses issues to determine a strategy going forward. Ellyce's diverse experience includes representing clients in internal investigations and government investigations along with responding to and coordinating crisis situations. Her client list includes notable companies from the healthcare, pharmaceutical, accounting, financial, defense and automotive industries. Ellyce earned her JD from the University of California, Los Angeles School of Law and her BA, *magna* cum laude, from the University of California Berkeley.

ALAN CHARLES RAUL

Sidley Austin LLP

Alan Raul is the founder and leader of Sidley Austin LLP's highly ranked privacy and cybersecurity practice. He represents companies on federal, state and international privacy issues, including global data protection and compliance programmes, data breaches, cybersecurity, consumer protection issues and internet law. He also advises companies on their digital governance strategies and cyber crisis management. Mr Raul's practice involves litigation and acting as counsel in consumer class actions and data breaches, as well as FTC, state attorney general, Department of Justice and other government investigations, enforcement actions and regulation. Mr Raul provides clients with perspective gained from extensive government service. He previously served as vice chair of the White House Privacy and Civil Liberties Oversight Board, general counsel of the Office of Management and Budget, general counsel of the US Department of Agriculture and associate counsel to the President. He currently serves as a member of the Technology Litigation Advisory Committee of the US Chamber Litigation Center (affiliated with the US Chamber of Commerce). Mr Raul also serves as a member of the American Bar Association's Cybersecurity Legal Task Force by appointment of the ABA president. He is also a member of the Council on Foreign Relations. Mr Raul holds degrees from Harvard College, Harvard University's Kennedy School of Government and Yale Law School.

© 2019 Law Business Research Ltd

SHERI PORATH ROCKWELL

Sidley Austin LLP

Sheri Porath Rockwell is a lawyer in the firm's Los Angeles office and a member of the privacy and cybersecurity practice and the complex commercial litigation practice. She advises clients on a variety of federal and state privacy issues, and is CIPP-US certified. Sheri earned her JD from the University of Southern California Gould School of Law and her BA, with honours, from the University of California, Berkeley.

SIDLEY AUSTIN LLP

1999 Avenue of the Stars, 17th floor
Los Angeles
California 90067
United States
Tel: +1 310 595 9500
Fax: +1 310 595 9501
ecooper@sidley.com

555 West Fifth Street, Suite 4000
Los Angeles
California 90013
United States
Tel: +1 213 896 6000
Fax: +1 213 896 6600
sheri.rockwell@sidley.com

1501 K Street, NW
Washington, DC 20005
United States
Tel: +1 202 736 8000
Fax: +1 202 736 8711
araul@sidley.com

www.sidley.com

© 2019 Law Business Research Ltd

an LBR business

ISBN 978-1-83862-062-2

© 2019 Law Business Research Ltd