THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

EIGHTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

EIGHTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2021
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Clare Bolton

HEAD OF BUSINESS DEVELOPMENT
Nick Barette

TEAM LEADERS
Joel Woods, Jack Bagnall

BUSINESS DEVELOPMENT MANAGERS
Rebecca Mogridge, Katie Hodgetts, Joey Kwok

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Georgia Goldberg

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Jonathan Allen

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

www.TheLawReviews.co.uk

ISBN 978-1-83862-810-9

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

ACKNOWLEDGEMENTS

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

ADVOKAADIBÜROO NORDX LEGAL

ALLENS

ANJIE LAW FIRM

ASTREA

AZEVEDO SETTE ADVOGADOS

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

BTS & PARTNERS

CLEMENS

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

K&K ADVOCATES

LEE, TSAI & PARTNERS

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

CONTENTS

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 2021: 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.

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.

The Framework consists of a set of privacy principles and implementation guidelines designed to balance APEC's goals of protecting privacy and facilitating the free flow of information among APEC economies to ensure continued trade and economic growth in the APEC region.[6] This principles-based approach allows for 'consistent rather than identical' privacy protections that reconcile the need for consumer privacy with business and commercial interests, while also recognising the 'cultural and other diversities' that exist within the member economies.[7] The Framework was modelled upon the OECD's Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data,[8] and was updated in 2015.[9]

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.

APEC's Cross-Border Privacy Rules (CBPR) system implements the APEC Framework as it applies to the flow of personal information across APEC member economies. Specifically, it is a government-backed data privacy certification that data controllers trading within APEC member economies can join to demonstrate their compliance with the APEC Privacy Framework's privacy principles. In 2015, APEC developed the Privacy Recognition for Processors (PRP) system, a corollary to the CBPR system for data processors. APEC continues to work with the EU to study the potential interoperability of the APEC and the EU's 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.

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)).

6 APEC Privacy Framework (2015), Foreword.

7 APEC Privacy Framework., Preamble, Paragraph 6.

8 https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).

9 https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).

II APEC PRIVACY FRAMEWORK

i Introduction

The APEC Privacy Framework, endorsed by APEC in 2005, consists of a set of principles intended to guide the development of information privacy protection in the Asia-Pacific region in a manner that ensures 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. The Framework was endorsed by leaders of different APEC 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. It 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.[10] 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.[11]

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 articulates basic principles of privacy protection and provides guidance for implementation domestically and internationally. A central tenant of the Framework is that privacy regulations must take into account the importance of business and commercial interests, as well as the 'cultural and other diversities' in member economies.[12] Its principles-based approach allows each economy to develop privacy laws that are 'consistent with but not identical' to privacy laws in other member economies, and that always take commercial interests into account.[13] The Framework cautions that when regulatory systems fail to account for business and industry and 'unnecessarily restrict' the flow of information, it results in 'adverse implications for global businesses, economies and individuals'.[14]

ii The Privacy Framework

The Privacy Framework has four parts:

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;

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

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

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

10 APEC Framework at pp. 3–4.

11 https://postcourier.com.pg/apec-privacy-framework-revised/.

12 APEC Privacy Framework, Paragraph 6.

13 APEC Privacy Framework, Paragraph 6.

14 APEC Privacy Framework, Paragraph 3.

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

Framework objectives

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, and thus the principles allow exceptions that will be consistent with particular domestic circumstances.[15] The Framework specifically recognises that there 'should be flexibility in implementing these Principles'.[16]

Scope of Framework – organisations and businesses

The Privacy Framework applies to businesses and organisations in the public and private sectors (referred to hereafter collectively as 'organisations') and individuals who control the 'collection, holding, processing, use, transfer or disclosure of personal information', including those who instruct others to do so on their behalf.[17] It does not apply to individuals who collect, hold, process or use personal information for personal, family or household purposes (e.g., address books, phone lists, or family newsletters).[18]

Scope of Framework – personal information

The 'personal information' encompassed by the Framework is defined as 'any information about an identified or identifiable individual'.[19] It includes information that may not be personally identifiable on its own, but when put together with other data, would identify an individual.[20] The Framework gives as an example metadata that, when aggregated, can reveal personal information and 'give an insight into an individual's behaviour, social relationships, private preferences and identity'.[21] Only the personal information of 'natural living persons' is in scope, meaning it does not apply to the personal information of deceased individuals or legal entities that may be elsewhere defined as 'persons'.

The Framework has 'limited application' to publicly available information, defined as information an individual 'knowingly makes or permits to be made available to the public'

15 See APEC Privacy Framework, Paragraph 18.
16 See APEC Privacy Framework, Paragraph 17.
17 APEC Privacy Framework, Paragraph 10.
18 APEC Privacy Framework, Paragraph 10.
19 APEC Privacy Framework, Paragraph 9.
20 APEC Privacy Framework, Paragraph 9.
21 APEC Privacy Framework, Paragraph 9.

and information that is 'legally obtained and accessed from government records that are available to the public, journalistic reports, or information required by law to be made available to the public'.[22]

The nine principles of the Privacy Framework (Part III)

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 organisational controls to prevent such harms be proportionate to the likelihood and severity of harm. When there has been a breach affecting personal information, this principle suggests that providing notice to the affected individual or enforcement authorities might reduce the risk of harmful consequences.[23]

Principle II – notice

The notice principle is designed to both provide transparency about the personal information collected about individuals and how it is being used and to also inform individuals about the choices and means they have to limit the use and disclosure of, and to access and correct, their personal information, including how to contact the controller about its personal information practices.[24] Towards that end, this principle directs that such disclosures be made at or before the time of collection, or as soon thereafter as is practicable, so that individuals can 'make an informed decision' about interacting with the controller.[25] Yet, it also recognises there are situations in which such notice is not necessary, such as in the exchange of business cards in the context of a business relationship where the parties would not expect to be given notice.[26]

22 APEC Privacy Framework, Paragraph 11.

23 APEC Privacy Framework, Paragraph 20.

24 APEC Privacy Framework, Paragraph 21.

25 APEC Privacy Framework, Paragraph 21.

26 APEC Privacy Framework, Paragraphs 21–23.

Principle III – collection limitation

This principle limits the collection of personal information to only that which is relevant to the purpose of collection, and should be done using 'lawful and fair' collection methods that do not include obtaining information under false pretences, even in those economies where there is no explicit law against doing so.[27] It also stresses that, where appropriate, information should be collected with notice to, or consent of, the data subject.[28]

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, and that such choices be 'clearly worded' to make it easily understandable to particular audiences (e.g., providing in relevant languages or using age-appropriate language), and are displayed 'clearly and conspicuously'.[29] This principle also contemplates that, in some instances, consent is neither necessary (e.g., when contact information exchanged in a business-to-business context) nor practicable (e.g., employers giving employees the choice to use their personal information for HR purposes).[30]

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, and to challenge and correct the accuracy of that information. If an organisation denies such access or correction requests, the principle also provides that the individual should be able to challenge such

27 APEC Privacy Framework, Paragraph 24.
28 APEC Privacy Framework, Paragraph 24.
29 APEC Privacy Framework, Paragraph 26.
30 APEC Privacy Framework, Paragraph 26.

denials. 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 would be violated.[31]

Principle IX – accountability

This principle requires that a data controller be accountable for complying with measures that give effect to the nine principles. When transferring personal information to another person or organisation, whether domestically or internationally, this principle states the controller should either obtain consent of the individual or exercise due diligence to ensure that recipients also protect the information in a manner that is consistent with the principles. Obtaining consent or conducting such due diligence is not required when domestic laws require disclosures of personal information.

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.

Implementation (Part IV)

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'.[32] 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.[33]

iii Data privacy individual action plans

Economies are, nevertheless, encouraged to keep others apprised of their domestic implementation of the Privacy Framework by completing and periodically updating Data Privacy Individual Action Plans (IAPs).[34] IAPs require economies to summarise provisions of their domestic privacy protection schemes that correspond to each of the Framework's privacy principles, describe enforcement mechanisms and remedies, and identify areas that need

31 APEC Privacy Framework, Paragraphs 29, 30.

32 See APEC Privacy Framework, Paragraph 37.

33 See APEC Privacy Framework, Paragraphs 53, 37.

34 https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group/Data-Privacy-Individual-Action-Plan at 'Explanatory Notes'.

further consideration or where the privacy protections are in 'draft' form.[35] IAPs are posted on the web page of APEC's Digital Economy Steering Group.[36] As of 2021, 14 member economies have IAPs.[37]

Without a central enforcement authority, though, it appears that most economies are not placing a high priority on updating their IAPs. As of July 2021, with the exception of Canada, none of the plans on APEC's web page had been updated in the last six years, and several of the IAPs dated back to 2006 (including the US plan).[38]

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)) to facilitate cross-border cooperation in investigation and enforcement.[39]

III APEC CROSS-BORDER DATA TRANSFER

i Data Privacy Pathfinder initiative

In 2007, APEC ministers endorsed the Data Privacy Pathfinder initiative to develop a system to provide for accountable cross-border data flows in the APEC region consistent with the Privacy Framework.[40] Thirteen APEC economies joined the Pathfinder when it began in 2007, and they were joined in 2008 by three additional economies.[41] Through the Pathfinder, nine different work streams, or projects, were developed to design, test and implement four essential elements of a cross-border privacy rule regime: self-assessment, compliance review, recognition or acceptance of the cross-border rules, and dispute resolution an enforcement.[42]

The Pathfinder's work resulted in the creation of APEC's Cross-Border Privacy Rules system and the Cross-Border Privacy Enforcement Arrangement, both discussed below.

ii The Cross-Border Privacy Rules system

The APEC Cross-Border Privacy Rules system, endorsed in 2011, provides a single framework for the exchange of personal information by organisations in APEC economies.[43] The system bridges different national privacy laws in the APEC region by certifying organisations as

35 See APEC Information Privacy Individual Action Plan – Canada (August 2019) at footnotes 1-4 (instructions for completing template Action Plan chart) found at https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group/Data-Privacy-Individual-Action-Plan.

36 https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group/Data-Privacy-Individual-Action-Plan.

37 See https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group/Data-Privacy-Individual-Action-Plan.

38 https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group/Data-Privacy-Individual-Action-Plan.

39 See APEC Privacy Framework, Paragraphs 57–64.

40 See https://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Privacy-Framework.aspx.

41 Hredzack, Tammy L and Gómez, Azul Ogazón, 'Enabling Electronic Commerce: The Contribution of APEC's Data Privacy Framework', APEC Policy Support Unit (October 2011) at pages 7–8.

42 Hredzack, Tammy L and Gómez, Azul Ogazón, 'Enabling Electronic Commerce: The Contribution of APEC's Data Privacy Framework', APEC Policy Support Unit (October 2011), pages 10–11.

43 http://cbprs.org/business/.

having privacy practices and procedures that meet APEC standards that are independent of individual national privacy regimes. The CBPR system adopts an 'accountability-based' approach whereby organisations are held to comply with CBPR principles, rather than comply with top-down regulation that may be ill-suited to an organisation's unique circumstances.[44] As of July 2021, nine APEC economies participate in the CBPR system – Canada, Japan, Mexico, South Korea, Singapore, the United States, Australia, Taiwan and the Philippines.[45]

Additional APEC member countries may join the CBPR system in the near future. China is in the process of updating its Personal Information Protection Law, and in May 2021 the Centre for Informational Policy Leadership provided comments, which included the recommendation that China join the CBPR system.[46]

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.[47]

The CBPR system is governed by the Data Privacy Subgroup, which administers the programme through the Joint Oversight Panel, an entity whose members are nominated representatives of participating economies in addition to members of working groups the Panel may establish. 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.[48] 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.[49]

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.[50] When an economy is certified, it means the CBPR's Joint Oversight Panel has determined the

44 http://cbprs.org/wp-content/uploads/2019/05/Benefits-of-CBPR-System-Guide_Jan-2019_FINAL.pdf.

45 http://cbprs.org/government/.

46 https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/english_-_cipl_comments_on_chinas_updated_draft_personal_information_protection_law__18_may_2021_.pdf.

47 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.

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

49 See www.cbprs.org.

50 http://cbprs.org/business.

economy's laws and regulations can be leveraged to enforce organisations' compliance with the CBPR programme requirements when organisations are operating from or within that economy's jurisdiction.[51]

The technical CBPR certification requirements for APEC member economies are as follows:

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

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.

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.[52]

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.[53]

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;

51 See http://cbprs.org/government/economies-requirements/ and linked Template Notice of Intent to Participate in CBPR System, Annex B.

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

53 http://cbprs.org/accountability-agents/new-agent-process/.

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.[54]

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 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.[55]

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.[56] As of July 2021, the CBPR system recognises eight accountability agents: TRUSTe, Schellman & Company, NCC Group, HITRUST, and BBB National Programs for the United States; Infocomm Media Development Authority for Singapore; Korea Internet and Security Agency; and JIPDEC for Japan.[57] Accountability agents for other countries have yet to be designated; however, Taiwan

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

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

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

57 http://cbprs.org/business/.

announced in June 2021 that it has received approval to establish an accountability agent, the Information Industry Promotion Council.[58] The CBPR system directory has yet to be updated to reflect this change.[59]

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 2021, 41 organisations have been CBPR certified, 35 of which have been certified in the United States, two in Japan, and four in Singapore. No Korean organisations have been certified as of August 2020.[60] Certifications often encompass subsidiaries that are located in countries other than the certifying country. Certified companies must undergo annual recertification, which the accountability agent reviews.

CBPR and 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. To be CBPR-certified, economies must be able to use their domestic laws to enforce organisations' agreements to abide by CBPR rules. If an APEC economy's domestic privacy laws are stronger than those of the CBPR system, then those laws will continue to apply to their full extent.

Participating economies may have domestic laws that govern the transfer of personal data across borders in addition to CBPR requirements. Other economies may allow cross-border transfers to organisations based only on the fact that they are CBPR-certified. For example, in June 2020, Singapore amended its Personal Data Protection Regulations to allow Singapore organisations to transfer data outside the country based only on the recipient's CBPR certification, removing the need to enter into additional data transfer agreements or binding corporate rules.[61] Similarly, in March 2021, the Office of the Privacy Commissioner for Bermuda announced that they will now recognise the APEC CBPR system as a certification mechanism that can be used for international data transfers under the Personal Information Protection Act.[62]

58 https://www.dataguidance.com/news/taiwan-ndc-announces-approval-establish-responsible.

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

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

61 https://www.pdpc.gov.sg/News-and-Events/Announcements/2020/06/Singapore-Now-Recognises-APEC-CBPR-and-PRP-Certifications-Under-PDPA.

62 https://www.privacy.bm/post/privcom-recognises-apec-cbpr-system-as-a-certification-mechanism-for-overseas-data-transfers.

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.[63] 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.[64] 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.[65]

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.[66] 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.[67]

As of August 2020, two APEC economies have joined the PRP system – the United States and Singapore – and PRP-certified accountability agents have been certified from each country.[68] Twenty-four processors have been certified under the programme, 22 of which are based in the United States, and two of which are based in Singapore.[69]

iii The Cross-border Privacy Enforcement Arrangement (CPEA)

One of the primary 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;

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

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

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

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

67 http://cbprs.org/wp-content/uploads/2020/08/PRP-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-1.pdf.

68 http://cbprs.org/documents/.

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

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.[70]

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 August 2020, CPEA participants included over two dozen Privacy Enforcement Authorities from 11 APEC economies.[71]

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.

IV 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 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, APEC has been cooperating with the EU since 2012 to study the interoperability of the APEC and EU data privacy regimes, focusing on mechanisms that can be used to facilitate cross-border data flows and data protection enforcement between the APEC region and the EU.[72]

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.[73] The study found that the CBPR system was a 'good example'

70 www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.

71 www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.

72 www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group/Data-Privacy-Subgroup-Meeting-with-European-Union.

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

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.[74] Future interoperability discussions will need to take into account the impact of the July 2020 *Schrems II* decision in the European Court of Justice, which cast doubt on mechanisms to transfer personal data from Europe to the United States, but has implications for all countries that receive personal data from the EU.

V THE YEAR IN REVIEW AND OUTLOOK

The APEC CBPR system saw modest growth in 2020–2021. In 2020, no new countries joined the APEC CBPR system.[75] In early 2021, one US accountability agent was certified.[76] This new accountability agent, BBN National Programs, is the first non-profit to be certified.[77] Between September 2020 and July 2021, eight additional companies have become CBPR certified; three in Singapore and five in the US.[78] During the same time period, eight additional companies have become PRP certified; two in Singapore and six in the US, including DocuSign and Talkdesk.[79] It is possible that the relatively slow pace at which organisations are choosing to become CBPR or PRP certified may impact the willingness of other large companies to invest in certification.

Also in 2020, APEC's CBPR system was recognised in the United States–Mexico–Canada Agreement as 'a valid mechanism to facilitate cross-border information transfers while protecting personal information'.[80] In 2021, the Bermuda Privacy Commissioner recognised the APEC CBPR system 'as a certification mechanism for overseas data transfers' that can be used according to the Personal Information Protection Act.[81]

No CBPR enforcement actions were brought in 2020, as governments in affected regions focused on matters relating to the global covid-19 crisis. Malaysia hosted an entirely virtual APEC Summit in 2020, and in 2021, New Zealand hosted the APEC Summit virtually.[82]

In March 2021, the APEC Data Privacy Subgroup released a statement on covid-19.[83] The statement emphasised the importance of data to the understanding of covid-19, tracking and containing the virus's spread, and developing treatments and vaccines.[84] The APEC Data Privacy Subgroup recognised the importance of cooperation within APEC to limit the global health and economic impact of covid-19 while reaffirming its commitment to the principles in the APEC Privacy Framework that aim to strengthen the economy and benefit the public while also maintaining appropriate data privacy.[85]

74 https://ec.europa.eu/info/sites/info/files/data_protection_certification_mechanisms_study_publish_0.pdf.
75 http://cbprs.org/government/.
76 http://cbprs.org/documents/.
77 https://www.huntonprivacyblog.com/2021/01/26/apec-endorses-the-first-u-s-non-profit-accountability-agent/.
78 http://cbprs.org/compliance-directory/cbpr-system/.
79 http://cbprs.org/compliance-directory/prp/.
80 United States–Canada-Mexico Trade Agreement (July 2020), Article 19.8, Paragraph 6.
81 https://www.privacy.bm/post/privcom-recognises-apec-cbpr-system-as-a-certification-mechanism-for-overseas-data-transfers.
82 https://www.apec2021nz.org/.
83 https://www.apec.org/Press/News-Releases/2021/0315_DPS.
84 https://www.apec.org/Press/News-Releases/2021/0315_DPS.
85 https://www.apec.org/Press/News-Releases/2021/0315_DPS.

Although the APEC CBPR system covers the world's largest and most dynamic marketplace, and promises to provide the opportunity to promote data flow across the world's largest single platform of its kind, the system has been described as 'an underperformer'[86] in comparison with, for instance, the GDPR. Part of the reason for this 'underperformance' is that, as outlined above, APEC member economies are not under any binding commitment to legislate domestically to adopt the APEC CBPR framework. Owing to the voluntary nature of the arrangements made by APEC, inevitably, member economies tend to take different approaches to data protection, especially since APEC member economies come from diverse cultures, histories as well as systems. Further, the trend of data localisation in Asia-Pacific, as represented by China and Vietnam, also undermines regional and international cooperative efforts on data privacy protection. As a result of these factors, adoption of the APEC CBPR system is progressing slowly. Looking ahead, as many international and regional efforts are stalled as a result of the covid-19 pandemic, we do not anticipate much significant development in APEC's data privacy protection efforts in the coming year; however, with APEC's COVID-19 Economic Response & Recovery Initiatives under way, improvements in privacy protection may become a priority again soon.

86 http://www.dgcs-research.net/a/Opinion/2018/0201/100.html.

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, defence 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.

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. She advises clients on a variety of federal and state privacy issues and is CIPP-US certified. Sheri serves as the acting chair of the California Lawyers Association's Privacy Law Section, which she helped found. She 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
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

an LBR business

ISBN 978-1-83862-810-9