

---

# THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

---

THIRD EDITION

EDITOR  
ALAN CHARLES RAUL

LAW BUSINESS RESEARCH

# THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

---

Third Edition

Editor  
ALAN CHARLES RAUL

LAW BUSINESS RESEARCH LTD

PUBLISHER  
Gideon Robertson

SENIOR BUSINESS DEVELOPMENT MANAGER  
Nick Barette

BUSINESS DEVELOPMENT MANAGER  
Thomas Lee

SENIOR ACCOUNT MANAGERS  
Felicity Bown, Joel Woods

ACCOUNT MANAGERS  
Jessica Parsons, Jesse Rae Farragher

MARKETING COORDINATOR  
Rebecca Mogridge

EDITORIAL ASSISTANT  
Gavin Jordan

HEAD OF PRODUCTION  
Adam Myers

PRODUCTION EDITOR  
Anne Borthwick

SUBEDITOR  
Anna Andreoli

CHIEF EXECUTIVE OFFICER  
Paul Howarth

Published in the United Kingdom  
by Law Business Research Ltd, London  
87 Lancaster Road, London, W11 1QQ, UK  
© 2016 Law Business Research Ltd  
[www.TheLawReviews.co.uk](http://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 is accurate as of October 2016, 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 – [gideon.roberton@lbresearch.com](mailto:gideon.roberton@lbresearch.com)

ISBN 978-1-910813-32-4

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

# THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND  
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND  
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

THE PUBLIC-PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

THE SPORTS LAW REVIEW

THE INVESTMENT TREATY ARBITRATION REVIEW

THE GAMBLING LAW REVIEW

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW

THE REAL ESTATE, M&A AND PRIVATE EQUITY REVIEW

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW

# ACKNOWLEDGEMENTS

---

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

ALLENS

ASTREA

BAKER & MCKENZIE - CIS, LIMITED

BOGSCH & PARTNERS LAW FIRM

CMS CAMERON MCKENNA GRESZTA I SAWICKI SP.K

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

GIANNI, ORIGONI, GRIPPO, CAPPELLI & PARTNERS

JUN HE LAW OFFICES

LEE & KO

MATHESON

NNOVATION LLP

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SIQUEIRA CASTRO – ADVOGADOS

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VIEIRA DE ALMEIDA & ASSOCIADOS, SP RL

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

# CONTENTS

---

<b>Chapter 1</b>	GLOBAL OVERVIEW ..... 1 <i>Alan Charles Raul</i>
<b>Chapter 2</b>	EUROPEAN UNION OVERVIEW ..... 6 <i>William RM Long, Géraldine Scali, Francesca Blythe and Alan Charles Raul</i>
<b>Chapter 3</b>	APEC OVERVIEW ..... 25 <i>Catherine Valerio Barrad, Ellyce R Cooper and Alan Charles Raul</i>
<b>Chapter 4</b>	AUSTRALIA ..... 38 <i>Michael Morris</i>
<b>Chapter 5</b>	BELGIUM ..... 51 <i>Steven De Schrijver and Thomas Daenens</i>
<b>Chapter 6</b>	BRAZIL ..... 64 <i>Daniel Pitanga Bastos de Souza and Bruno Granzotto Giusto</i>
<b>Chapter 7</b>	CANADA ..... 73 <i>Shaun Brown</i>
<b>Chapter 8</b>	CHINA..... 89 <i>Marissa (Xiao) Dong</i>
<b>Chapter 9</b>	FRANCE ..... 100 <i>Dominique de Combles de Nayves &amp; Pierre Guillot</i>
<b>Chapter 10</b>	GERMANY..... 113 <i>Jens-Marwin Koch</i>



<b>Chapter 11</b>	HONG KONG.....	127
	<i>Yuet Ming Tham</i>	
<b>Chapter 12</b>	HUNGARY.....	142
	<i>Tamás Gödölle</i>	
<b>Chapter 13</b>	INDIA .....	159
	<i>Aditi Subramaniam</i>	
<b>Chapter 14</b>	IRELAND.....	170
	<i>Andreas Carney and Anne-Marie Bohan</i>	
<b>Chapter 15</b>	ITALY .....	184
	<i>Daniele Vecchi and Melissa Marchese</i>	
<b>Chapter 16</b>	JAPAN .....	199
	<i>Tomoki Ishiara</i>	
<b>Chapter 17</b>	KOREA.....	215
	<i>Kwang Bae Park and Ju Bong Jang</i>	
<b>Chapter 18</b>	MALAYSIA .....	229
	<i>Shanthi Kandiah</i>	
<b>Chapter 19</b>	MEXICO .....	242
	<i>César G Cruz-Ayala and Diego Acosta-Chin</i>	
<b>Chapter 20</b>	POLAND.....	256
	<i>Tomasz Koryzma, Marcin Lewoszewski, Agnieszka Besiekierska and Adriana Zdanowicz-Leśniak</i>	
<b>Chapter 21</b>	PORTUGAL .....	271
	<i>Magda Cocco, Inês Antas de Barros and Sofia de Vasconcelos Casimiro</i>	
<b>Chapter 22</b>	RUSSIA.....	282
	<i>Elena Kukushkina, Georgy Mzhavanadze and Vadim Perevalov</i>	

<b>Chapter 23</b>	SINGAPORE.....	294
	<i>Yuet Ming Tham</i>	
<b>Chapter 24</b>	SPAIN.....	310
	<i>Leticia López-Lapuente and Reyes Bermejo Bosch</i>	
<b>Chapter 25</b>	SWITZERLAND.....	322
	<i>Jürg Schneider and Monique Sturny</i>	
<b>Chapter 26</b>	TURKEY .....	341
	<i>Gönenç Gürkaynak and İlay Yılmaz</i>	
<b>Chapter 27</b>	UNITED KINGDOM .....	352
	<i>William RM Long, Géraldine Scali and Francesca Blythe</i>	
<b>Chapter 28</b>	UNITED STATES.....	370
	<i>Alan Charles Raul, Tasha D Manoranjan and Vivek K Mohan</i>	
<b>Appendix 1</b>	ABOUT THE AUTHORS.....	403
<b>Appendix 2</b>	CONTRIBUTING LAW FIRMS' CONTACT DETAILS.....	419

## Chapter 3

---

# APEC OVERVIEW

*Catherine Valerio Barrad, Ellyce R Cooper and Alan Charles Raul<sup>1</sup>*

### I OVERVIEW

Asia-Pacific Economic Cooperation (APEC) is an organisation of economic entities in the Asia-Pacific region formed to enhance economic growth and prosperity in the region. It was established in 1989 by 12 Asia-Pacific economies as an informal ministerial-level dialogue group. 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’. Since 1993, the heads of the member economies have met annually at an APEC Economic Leaders Meeting, which has since grown to include 21 member economies as of August 2016: 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.<sup>2</sup> Collectively, the 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.<sup>3</sup>

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. 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 recognition of the exponential growth and transformative nature of electronic commerce, and its contribution to economic

---

1 Ellyce R Cooper and Alan Charles Raul are partners at Sidley Austin LLP. Catherine Valerio Barrad was formerly a partner at Sidley, and is now university counsel for the California State University System.

2 The current list of APEC member economies can be found at [www.apec.org/About-Us/About-APEC/Member-Economies.aspx](http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx).

3 See [www.statistics.apec.org](http://www.statistics.apec.org).

growth in the region, APEC established an Electronic Commerce Steering Group (ECSG) in 1999, which began to work toward the development of consistent legal, regulatory and policy environments in the Asia-Pacific area.<sup>4</sup> It further established the Data Privacy Subgroup under the ECSG in 2003 to address privacy and other issues identified in the 1998 APEC Blueprint for Action on Economic Commerce.<sup>5</sup>

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 (and thus promoting electronic commerce). The result was the principles-based APEC Privacy Framework, which was endorsed by the APEC economies in 2004. Although consistent with the original 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.

APEC recently developed 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 EU data privacy regimes, and in 2014 issued a joint referential document that maps the requirements of the two regimes for the benefit of businesses that seek certification or approval under both systems. A common questionnaire and a referential document for processors are also under development.

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

## **II APEC PRIVACY FRAMEWORK**

### **i Introduction**

The APEC Privacy Framework was developed to promote a consistent approach to information privacy protection in the Asia-Pacific region as a means of ensuring the free flow

---

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 [...] and consumer protection'. See APEC Privacy Framework, at 2 (available at [www.apec.org/Groups/Committee-on-Trade-and-Investment/-/media/Files/Groups/ECSG/05\\_ecsg\\_privacyframewk.ashx](http://www.apec.org/Groups/Committee-on-Trade-and-Investment/-/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx)).

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. This recognition was the impetus behind the development of the Privacy Framework. Thus, the APEC 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 adoption of 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 for 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.

## 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 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 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, the Framework 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.<sup>6</sup> The Framework specifically recognises that there 'should be flexibility in implementing these Principles'.<sup>7</sup>

---

6 See APEC Privacy Framework, Paragraph 13.

7 See APEC Privacy Framework, Paragraph 12.

### *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 APEC Privacy Framework was based on the original OECD Guidelines. The APEC privacy principles address personal information about living individuals, and exclude both publicly available information and information connected with domestic affairs. The principles apply to persons or organisations in both public and private sectors who control the collection, holding, processing or use of personal information. Organisations that act as agents for others are excluded from compliance.

While based on the OECD Guidelines, the APEC principles 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 4 regarding use of information. The APEC principles also permit a broader scope of exceptions and are slightly stronger than the OECD Guidelines on notice. In general, the APEC principles reflect the objective of promoting economic development, and the respect for differing legal and social values among the 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 addresses the information that a data controller must include in a notice to individuals when collecting their personal information. It also requires that all reasonable steps be taken to provide the notice either before or at the time of collection, and if not, then as soon after collection as is reasonably practicable. The principle further provides for an exception for notice of collection and use of publicly available information.

#### *Principle III – collection limitation*

This principle provides for the lawful and fair collection of personal information limited to that which is relevant to the purpose of collection and, where appropriate, with notice to, or consent of, the data subject.

#### *Principle IV – uses of personal information*

This principle limits the use of personal information to those uses that fulfil the purpose of collection and other compatible or related purposes. It includes exceptions for information collected with the consent of the data subject, and collection necessary to complete a request of the data subject or as required by law.

#### *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 maintained 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 such safeguards be periodically reassessed.

*Principle VIII – access and correction*

The access and correction principle directs that individuals have the right of access to their personal information within a reasonable time and in a reasonable manner, and may challenge its accuracy 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 privacy rights of other data subjects 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 the 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 that 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 Framework.

*Implementation (Part IV)*

Because APEC is a cooperative organisation, 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 methods’.<sup>8</sup> The Framework advocates ‘an appropriate array of remedies [...] commensurate with the extent of the actual or potential harm’ and supports a choice of remedies appropriate to each member economy. 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

---

8 See APEC Privacy Framework, Paragraph 31.

research, and to engage in cross-border cooperation in investigation and enforcement.<sup>9</sup> This concept later developed into the Cross-Border Privacy Enforcement Arrangement (CPEA – see Section III.iii, *infra*).

### **iii Data privacy individual action plans (IAPs)**

Data privacy IAPs are periodic, national reports to APEC on each member economy's progress of adopting the Privacy Framework domestically. IAPs are the mechanism of accountability by member economies to each other for implementation of the APEC Privacy Framework.<sup>10</sup> The IAPs are periodically updated as the Privacy Framework is implemented within each such economy. As of 2016, 14 member economies have posted IAPs on the APEC website.<sup>11</sup>

## **III APEC CROSS-BORDER DATA TRANSFER**

### **i Data Privacy Pathfinder initiative**

The APEC Privacy Framework does not explicitly address the issue of cross-border data transfer, but rather calls for cooperative development of cross-border privacy rules.<sup>12</sup> 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 rules, and to implement an accountable cross-border privacy system. Since 2008, the Data Privacy Subgroup has been working on nine interrelated projects to support the development of cross-border privacy rules in the Asia-Pacific region. Both the CBPR system and the CPEA are outcomes of the Pathfinder initiative.

### **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 a newly established system, the CBPR system is in early stages of implementation. As of August 2016, four APEC economies participate in the CBPR system – Canada, Japan, Mexico and the United States – with more expected to join.

In general, the CBPR system requires businesses to develop their own internal privacy-based rules governing the transfer of personal data across borders under standards

---

9 See APEC Privacy Framework, Paragraphs 40–45.

10 See APEC Privacy Framework, Paragraph 39.

11 See [www.apec.org/Groups/Committee-on-Trade-and-Investment/-/link.aspx?\\_id=CB717EE6184848D396F31DBB814E5C90&\\_z=z](http://www.apec.org/Groups/Committee-on-Trade-and-Investment/-/link.aspx?_id=CB717EE6184848D396F31DBB814E5C90&_z=z).

12 See APEC Privacy Framework, Paragraphs 46–48.



that meet or exceed the APEC Privacy Framework. The 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 the goals of the CBPR system is to 'lift the overall standard of privacy protection throughout the [Asia-Pacific] region' through voluntary, enforceable standards set out within it.<sup>13</sup>

Organisations that choose to participate in the CBPR system must submit their privacy practices and policies for evaluation by an APEC-recognised accountability agent to assess compliance with the programme. Upon certification, the practices and policies will become binding on that organisation and enforceable through the relevant privacy enforcement authority.<sup>14</sup>

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 System Joint Oversight Panel and the Protocols of the APEC Cross-Border Privacy Rules System Joint Oversight Panel.<sup>15</sup>

Accountability agents and privacy enforcement authorities are responsible for enforcing the CBPR programme requirements, either under contract (private accountability agents) or under applicable domestic laws and regulations (accountability agents and privacy enforcement authorities).

The CBPR system has its own website, which includes general information about the system, charters and protocols, lists of current participants and certified entities, submissions and findings reports, and template forms.<sup>16</sup>

### *Participation in the CBPR system*

Only APEC member economies may participate in the CBPR system and must meet three requirements:

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

---

13 See [www.cbprs.org/Government/GovernmentDetails.aspx](http://www.cbprs.org/Government/GovernmentDetails.aspx).

14 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.

15 See [cbprs.blob.core.windows.net/files/JOP%20Charter.pdf](http://cbprs.blob.core.windows.net/files/JOP%20Charter.pdf); and also [cbprs.blob.core.windows.net/files/JOP%20Protocols.pdf](http://cbprs.blob.core.windows.net/files/JOP%20Protocols.pdf).

16 See [www.cbprs.org/default.aspx](http://www.cbprs.org/default.aspx).

- details regarding relevant domestic laws and regulations, enforcement entities and enforcement procedures; and
- c* 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.

### *Accountability agents*

The APEC CBPR system uses APEC-recognised accountability agents to review and certify participating organisations' privacy policies and practices as compliant with the APEC CBPR system requirements, including the APEC Privacy Framework. Applicant organisations may participate in the CBPR system only upon such certification, and it is the responsibility of the relevant accountability agent to undertake certification of an applicant organisation's compliance with the programme requirements. An accountability agent makes no determination as part of the CBPR verification programme regarding whether the applicant organisation complies with domestic legal obligations that may differ from the CBPR system requirements.

APEC CBPR system requirements for accountability agents 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;<sup>17</sup>
- 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.<sup>18</sup>

Proposed accountability agents are nominated by an APEC member economy and, following an application and review process by the Joint Oversight Panel, may be approved by the ECSG upon recommendation by the Panel. Any APEC member economy may review the recommendation as to any proposed accountability agent and present objections to the ECSG. Once an application has been approved by the ECSG, the accountability agent is deemed 'recognised'. 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.

No accountability agent may have an actual or potential conflict of interest, nor may it provide services to entities it has certified or that have applied for certification. It must continue to monitor certified organisations for compliance with the APEC CBPR system standards, and must obtain annual attestations regarding such compliance. It must publish

---

17 See [cbprs.blob.core.windows.net/files/Accountability%20Agent%20Recognition%20Criteria.pdf](https://cbprs.blob.core.windows.net/files/Accountability%20Agent%20Recognition%20Criteria.pdf).

18 See [cbprs.blob.core.windows.net/files/Signature%20and%20Contact%20Information.pdf](https://cbprs.blob.core.windows.net/files/Signature%20and%20Contact%20Information.pdf).

its certification standards and must promptly report all newly certified entities, as well as any suspended or terminated entities to the relevant privacy enforcement authorities and the CBPR Secretariat.

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.

Accountability agents are responsible for ensuring that any non-compliance is remedied in a timely fashion and reported, if necessary, to relevant enforcement authorities.

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.<sup>19</sup>

As of August 2016, the CBPR system recognises two accountability agents: TRUSTe and the Japan Institute for Promotion of Digital Economy and Community. TRUSTe is recognised to certify only organisations subject to the jurisdiction of the United States Federal Trade Commission (FTC). The Japan Institute for Promotion of Digital Economy and Community is recognised to certify organisations under the jurisdiction of the Ministry of Economy, Trade and Industry Government of Japan.

### *CBPR system compliance certification for organisations*

Only organisations that are subject to the laws of one or more APEC CBPR system participating economies are eligible for certification regarding personal information transfers between economies.

An organisation that chooses to participate in the CBPR system initiates the process through submission of a self-assessment questionnaire and relevant documentation to an APEC-recognised accountability agent. The accountability agent will then undertake an iterative evaluation process to determine whether the organisation meets the baseline standards of the programme. The accountability agent has sole responsibility for these first two phases of the CBPR system accreditation process (self-assessment and compliance review).

Organisations that are found to be in compliance with the programme requirements will be certified as CBPR-compliant and identified on the CBPR website. As of August 2016, more than 15 organisations have been APEC CBPR certified, all of which are in the United States, with more in various stages of review.<sup>20</sup> Certified companies must undergo annual recertification. As more accountability agents are recognised in the economies participating in the CBPR system, the number of certified organisations is expected to grow.

---

19 See [www.cbprs.org/Agents/AgentDetails.aspx](http://www.cbprs.org/Agents/AgentDetails.aspx).

20 A current list of APEC-certified organisations can be found at [cbprs.blob.core.windows.net/files/APEC%20CBPR%20Compliance%20Directory\\_Aug\\_15\\_2016.pdf](http://cbprs.blob.core.windows.net/files/APEC%20CBPR%20Compliance%20Directory_Aug_15_2016.pdf).

### *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, who remain responsible for the activities conducted by processors on their behalf, 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, which is a mechanism by which data processors can be certified by an accountability agent.<sup>21</sup> Such certification can provide assurances to APEC economies and data controllers regarding the quality and compatibility of the processor's privacy policies and practices. The PRP does not change the allocation of responsibility for the processor's practices to the data controller, and there is no requirement that a controller engage a PRP-recognised processor to comply with the Framework's accountability principle.

APEC is in the process of integrating the PRP system into the CBPR governance system, and it is expected that the PRP system will follow the same model. Differences in national laws among APEC economies, however, necessarily result in different enforceability options under the PRP system, and how each economy will support enforcement is not yet finalised.

### **iii The 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.

---

21 The PRP Purpose and Background Document can be found at [cbprs.blob.core.windows.net/files/PRP%20-%20Purpose%20and%20Background.pdf](https://cbprs.blob.core.windows.net/files/PRP%20-%20Purpose%20and%20Background.pdf); and the intake questionnaire for processors is at [cbprs.blob.core.windows.net/files/PRP%20-%20Intake%20Questionnaire.pdf](https://cbprs.blob.core.windows.net/files/PRP%20-%20Intake%20Questionnaire.pdf).

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 2016, CPEA participants included over two dozen Privacy Enforcement Authorities from nine APEC economies.<sup>22</sup>

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 – the APEC Privacy Framework and the EU Data Protection Directive – in 2012 APEC endorsed participation in a working group to study the interoperability of the APEC and EU data privacy regimes.

In early 2014, the APEC/EU Working Group released a reference document (endorsed by APEC Senior Leaders in February 2014) that maps the CBPR system requirements and the binding corporate rules under the EU Data Protection Directive, and identifies commonalities and differences between the two (Referential).<sup>23</sup> This document provides an important tool to multinational companies in developing global privacy compliance procedures that are compliant with both systems. Because it is set up in a block format, laying out the areas of commonality and the additional requirements of each privacy regime, the Referential provides a comparative tool that can be used as a checklist by companies seeking or considering certification by one or both systems. It does not, however, create interoperability or mutual recognition of the regimes.

---

22 See [www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx](http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx) for the most recent information about the CPEA and its participating privacy enforcement authorities.

23 See [www.apec.org/-/media/Files/Groups/ECSG/20140307\\_Referential-BCR-CBPR-reqs.pdf](http://www.apec.org/-/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf).

The Referential points out that such companies still need to be approved by each of the respective bodies in both EU Member States and APEC economies. The Referential further cautions against using the document itself as an organisation's proposed framework, because each organisation's privacy policies should be tailored to that organisation. Moreover, data processed in an APEC economy is still subject to that economy's domestic laws. And whenever the APEC CBPR system is incompatible with the EU Data Protection Directive, the organisation must affirmatively describe the circumstances under which it will apply the rules of one system rather than the other.

Following the Referential, the Article 29 Working Party and the APEC Data Privacy Subgroup agreed to develop additional practical tools to help organisations to become certified under both the BCR and CBPR systems. The joint working group has committed to developing a common application form based on each system's intake questionnaires that can be submitted, along with a mapping of the company policies and associated personal data and privacy programme practices and effectiveness tools, to support certification in both systems. The joint working group will also work, over the long term, to develop a common Referential for mapping requirements for processors under the BCR and CBPR systems.

The Referential and the common application are important steps towards developing policies, practices and enforcement procedures that could apply to both systems, and perhaps – eventually – a common framework.

## **V THE YEAR IN REVIEW AND OUTLOOK**

The Data Privacy Subgroup is undertaking a 10-year review and evaluation (stocktake) of domestic and international implementation of the APEC Privacy Framework through a working group established for that purpose and led by Australia. The member economies have been encouraged to update their IAPs in support of that stocktake. The stocktake will consider whether the APEC Privacy Framework should be updated to ensure relevance as the market evolves with technology innovations, such as big data, cloud computing and the internet of things. It will consider updating the Framework by addressing such topics as interoperability with other privacy frameworks, breach notifications, privacy management programmes and factors to consider when balancing economic and privacy interests.

On 15 April 2015, Canada joined the United States (2012), Mexico (2013) and Japan (2014) as an approved APEC economy participating in the APEC CBPR system. This system is growing slowly, as some economies are waiting to see interest from business, and some businesses are waiting for member economies to join. With all of the North American Free Trade Agreement countries participating, the CBPR system has made an important step towards an international presence, which may encourage more APEC member economies and business organisations to participate. IBM became the first company to be certified under the APEC CBPR system, in August 2013; it has been joined by nearly two dozen others, including companies with significant international presence, such as Apple, HP and Merck. All of these companies were certified by TRUSTe, the sole accountability agent at the time.

TRUSTe became the first recognised accountability agent under the CBPR system on 25 June 2013, and that status was renewed unanimously by the 21 APEC member economies in early 2015. In early 2016, the 21 APEC member economies approved the Japan Institute for Promotion of Digital Economy and Community (now called JIPDEC) as Japan's accountability agent. Mexico and Canada have not yet identified their domestic accountability agents.

The FTC has started to bring enforcement actions under APEC. On 29 June 2016, the FTC issued a no-fault consent order in its first enforcement decision under the CBPR against Very Incognito Technologies Inc for misrepresenting its compliance with the CBPR.<sup>24</sup> Very Incognito Technologies, while operating as Vipvape, deceptively advertised that it complied with the CBPR without undergoing the appropriate review. The FTC held Vipvape is 'prohibited from misrepresenting its participation, membership or certification in any privacy or security program sponsored by a government or self-regulatory organization'. On 14 July 2016, the FTC announced that it had sent warnings letters to 28 companies who claim compliance with the CBPR, despite their failure to meet the CBPR requirements.<sup>25</sup> The combination of the first enforcement action and the large number of enforcement letters indicates that the FTC may play a more active role in the future enforcement of the CBPR.

On 1 March 2016, Merck became the first US-based company to successfully use its CBPR certification as the foundation for its application to the CBPR.<sup>26</sup>

On 12 July 2016, the EU adopted the EU–US Privacy Shield. The purpose of the Privacy Shield is to provide rights to EU citizens whose personal data is transferred to the US and clarify the requirements for businesses performing transatlantic data transfers. US companies transferring data into the European market should look to both the EU–US Privacy Shield and APEC'S CBPR for guidance.

---

24 See *In re Very Incognito Tech, Inc*, FTC, No. 162 3034, final order, 6/29/16.

25 See [www.law360.com/articles/817584/ftc-sends-warnings-to-cos-over-apec-privacy-compliance](http://www.law360.com/articles/817584/ftc-sends-warnings-to-cos-over-apec-privacy-compliance).

26 See [www.troutmansanders.com/2016-spring-update-on-us-eu-privacy-shield-program-04-11-2016](http://www.troutmansanders.com/2016-spring-update-on-us-eu-privacy-shield-program-04-11-2016).

## Appendix 1

---

# ABOUT THE AUTHORS

### **CATHERINE VALERIO BARRAD**

*Sidley Austin LLP*

Catherine M Valerio Barrad is university counsel for the California State University System. She previously served as a partner in the Los Angeles office of Sidley Austin LLP.

### **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 practice. Ellyce has extensive experience 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 lead global coordinator of Sidley Austin LLP's highly ranked privacy, data security and information law 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. 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 Data Security, Privacy & Intellectual Property Litigation Advisory Committee of the US Chamber Litigation Center (affiliated with the US Chamber of Commerce). Mr Raul has also served on the American Bar Association's Cybersecurity Legal Task Force, by appointment of the ABA President, and currently remains an *ex officio* member. 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.

**SIDLEY AUSTIN LLP**

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