October 2020
2nd Edition

APEC CBPR & PRP

Questions and Answers

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

This document addresses some commonly asked questions about the APEC Cross-Border Privacy Rules (CBPR) [1] and Privacy Recognition for Processors (PRP) [2] systems.

Frequently Asked Questions

1. What is APEC?

2. What are the APEC Cross-Border Privacy Rules (CBPR)?

3. Which APEC economies participate in the CBPR?

4. What is the APEC Privacy Recognition for Processors (PRP)?

5. How can companies become CBPR or PRP certified?

6. What are CBPR Program Requirements?

7. What is an "Accountability Agent"?

8. How do APEC economies join the CBPR and PRP systems?

9. Are the CBPR and PRP enforceable?

10. What is the APEC Cross-Border Privacy Enforcement Arrangement (CPEA)?

11. How do CBPR and PRP interact with domestic privacy laws?

12. What happens if companies don't comply with their certification?

13. Why should companies seek CBPR or PRP certification?

14. How do CBPR help consumers?

15. How do CBPR help data protection authorities?

16. Can non-APEC economies join the CBPR and PRP systems?

17. Can companies based in non-APEC economies obtain CBPR and PRP certification?

18. Could there be interoperability between the CBPR and EU mechanisms like Binding Corporate Rules (BCR) and GDPR certifications?

19. Where can I find more information?

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

1. What is APEC?

The Asia-Pacific Economic Cooperation (APEC) is a regional forum established in 1989 dedicated to economic development and integration among member economies. Its members are: Australia; Brunei Darussalam; Canada; Chile; People's Republic of China; Hong Kong, China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; Philippines; Russia; Singapore; Chinese Taipei; Thailand; United States; and Vietnam.

APEC works through committees, working groups and projects on a wide range of policy issues related to the economy and trade. One of APEC's significant areas of focus has been data protection and privacy, which it has pursued mainly through its Digital Economy Steering Group (DESG) (formerly the Electronic Commerce Steering Group (ECSG)) and its Data Privacy Subgroup (DPS).

2. What are the APEC Cross-Border Privacy Rules (CBPR)?

The CBPR are a comprehensive privacy certification that provides organizations with a mechanism for cross-border data transfers—much like Binding Corporate Rules (BCR) in the EU, but with a broader scope. CBPR can be used for intra-company transfers, for transfers between unaffiliated companies, as well as for transfers to non CBPR-certified companies anywhere in the world. The CBPR comprise a set of 50 Program Requirements that operationalize the nine Privacy Principles set forth in the 2005 APEC Privacy Framework [3]. CBPR can be used not only as a cross-border transfer mechanism but also as a comprehensive domestic privacy compliance and accountability program.

3. Which APEC economies participate in the CBPR?

Nine APEC economies have joined the CBPR System to date—the United States, Mexico, Canada, Japan, South Korea, Singapore, Chinese Taipei, Australia and the Philippines. Several others are actively considering or working towards joining (e.g. Indonesia, Chile, Vietnam and Malaysia). All 21 APEC economies have endorsed the CBPR and have stated their intentions to joining at some point. After an economy joins the CBPR system, it must implement and operationalize it. The CBPR have been fully implemented and operationalized in the United States, Japan, South Korea and Singapore. The other participating economies are at varying stages of implementation and operationalizing.

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

4. What is the APEC Privacy Recognition for Processors (PRP)?

The PRP are a companion certification to the CBPR designed specifically for data processors that process personal data on behalf of data controllers. APEC created the PRP in 2015. The PRP have fewer Program Requirements than the CBPR and focus mostly on data security and the ability to implement the relevant CBPR requirements and other data privacy instructions of the controller. Their main purpose is to serve as a due diligence tool for data controllers that are looking for qualified data processors. Currently, the United States and Singapore are participating in the PRP, but other APEC economies are expected to follow.

5. How can companies become CBPR or PRP certified?

At present, companies must apply to a recognized APEC Accountability Agent, which is a third-party certification body within an APEC economy that has formally joined the CBPR system. A company must be certified in the participating APEC economy in which it is "primarily located" in the region. A company that is "primarily located" in an APEC economy can include all or some of its global corporate affiliates in the certification. It is important to note, however, that representatives from the nine CBPR participating economies are currently discussing possible models for how the CBPR and PRP systems could potentially be globalized to allow participation by non-APEC members as equal participants through the establishment of the CBPR system in a separate forum. Organizations could then apply to a recognized Accountability Agent in a participating country in which it is primarily located even if that country is not an APEC economy.

The Accountability Agent will evaluate whether the company's privacy policies and practices comply with the CBPR (or PRP) Program Requirements and will assist the company to come into compliance with them if they do not. Once the company is certified, complying with the CBPR (or PRP) becomes an enforceable obligation. The certification is subject to annual recertification.

6. What are CBPR Program Requirements?

The CBPR Program Requirements are the 50 privacy requirements to which companies must adhere and must implement in order to be certified under the CBPR. These 50 requirements operationalise the nine APEC Privacy Principles. During the certification process, Accountability Agents use a set of specific assessment criteria associated with each of these Program Requirements to assess the privacy policies and practices of the applicants. A similar process applies to the PRP.

7. What is an "Accountability Agent"?

Organizations certify to the CBPR (or PRP) through an approved third-party certification body known as an "Accountability Agent" in the jurisdiction in which the company is "primarily located". At present, organizations must certify in the jurisdiction where they are "primarily located" in the APEC region but if the CBPR and PRP systems are globalized then it would be possible to certify in any participating jurisdiction where the company is "primarily located", regardless of whether that is an APEC economy or not. Currently, there are seven operational CBPR Accountability Agents [4]. Several of the participating economies are still in the process of identifying their Accountability Agents. Until an Accountability Agent has been identified in an economy, companies "primarily located" in that economy cannot get certified.

8. How do APEC economies join the CBPR and PRP systems?

APEC has developed a process for its member economies to join the CBPR system. This process includes:

- A formal statement of intent to join the system by the government of the applying economy.
- Identifying at least one Accountability Agent that will be responsible for certifying businesses in that economy.
- Having at least one Privacy Enforcement Authority (PEA) capable of enforcing the CBPR join the APEC Cross-Border Privacy Enforcement Arrangement (CPEA).

Applications are vetted through a process involving the APEC Joint Oversight Panel (which was created for CBPR administration purposes) and the APEC Digital Economy Steering Group (DESG) and its Data Privacy Subgroup (DPS).

9. Are the CBPR and PRP Enforceable?

Yes. Once an organization joins the system and is certified by a third-party Accountability Agent under the CBPR Program Requirements, the certification becomes legally enforceable by the Privacy Enforcement Authority (PEA) in the economy in which the organization has been certified. To join the CBPR system, APEC economies must demonstrate that the CBPR are enforceable under their laws and by their PEA. Enforcement of the CBPR is currently provided by APEC-based Privacy Enforcement Authorities that have joined the APEC Cross-Border Privacy Enforcement Arrangement (CPEA). If the CBPR were to be globalized, the CPEA would have to be expanded to allow participation by PEAs from non-APEC economies. Organizations can certify to the CBPR only if they are subject to the enforcement jurisdiction of the PEA in the economy in which they seek certification.

10. What is the APEC Cross-Border Privacy Enforcement Arrangement (CPEA)?

The CPEA is an enforcement cooperation arrangement between Privacy Enforcement Authorities (PEAs) in APEC member economies. As noted above, however, if the CBPR were to be globalized, the CPEA would have to be expanded to allow participation by PEAs from non-APEC economies. The current participants are 26 PEAs from 10 APEC member economies [5]. The CPEA was created to ensure cross-border enforcement cooperation of the CBPR among participating APEC economies. However, it enables enforcement cooperation on all data protection and privacy-related enforcement matters, not just CBPR enforcement.

11. How do CBPR and PRP interact with domestic privacy laws?

The CBPR do not replace domestic privacy laws or other laws. In addition to complying with the CBPR Program Requirements, CBPR-certified organizations must also comply with domestic privacy laws. CBPR are enforceable under the domestic laws of participating economies. When a CBPR certified organization transfers covered personal data across borders, it must apply the CBPR protections plus any additional domestic requirements.

12. What happens if companies don't comply with their certification?

Certified organizations are required to have effective privacy complaint and redress mechanisms to address customer complaints concerning CBPR violations. In addition, companies that don't comply with their certification are subject to sanctions by their certifying Accountability Agent, including suspension or withdrawal of the certification. They are also subject to enforcement action by the Privacy Enforcement Authority in the jurisdiction in which they certified.

13. Why should companies seek CBPR or PRP certification?

There are many benefits in certifying to the CBPR:

- **Facilitates Data Transfers**: In an increasing number of APEC economies, they can serve as a formally recognized cross-border transfer mechanism for personal data. If the CBPR system is expanded beyond APEC, organizations will have access to certification under the first global data protection transfer mechanism.
- **Enables Compliance**: They provide a comprehensive privacy management program that can enable compliance with domestic privacy law as well as with other internationally recognized privacy standards.

- **Assists SMEs**: They can be particularly helpful for SMEs that may lack the expertise, staff or resources to devise their own comprehensive privacy programs.
- **Due Diligence Tool**: They can serve as a due diligence and risk management tool for companies seeking qualified third-party vendors, processors and business partners.
- **Demonstrates Privacy Accountability**: Participation in privacy certifications such as the CBPR and PRP can demonstrate corporate digital responsibility to consumers, potential business partners and Privacy Enforcement Authorities and increase their trust in the certified company.
- **Mitigating Factor in Enforcement**: They can serve as a mitigation factor in enforcement contexts where privacy laws allow consideration of good faith compliance efforts (such as participation in privacy codes of conduct and certifications) in enforcement and fine-setting decisions.

14. How do CBPR help consumers?

Having undergone a certification review process (and re-certifying on an annual basis) ensures that a company has an effective privacy program in place that meets the high standard of the CBPR. This results in stronger and more effective and consistent privacy protections for consumers. Also, the CBPR provide complaint and dispute resolution mechanisms for consumers that might otherwise not be available.

15. How do CBPR help data protection authorities?

Having a comprehensive privacy program that can be demonstrated on request enables more streamlined and efficient privacy investigations and enforcement actions. Thus, formal accountability and compliance programs like the CBPR can make enforcement matters less costly and time-intensive for both the enforcement authority and the company. In addition, the CBPR require organizations to have formal dispute resolution mechanisms, which can help relieve the burden on enforcement authorities associated with handling individual complaints. Also, to the extent privacy certifications raise the general level of privacy compliance, there may be fewer enforcement actions necessary.

16. Can non-APEC economies join the CBPR and PRP systems?

Not currently. However, APEC economies participating in the CBPR are discussing possible models for expanding the reach of the CBPR given the interest among industry and other stakeholders to have a global solution for cross-border data transfers. Moreover, participating economies are giving thought to how such an expansion will be beneficial for and contribute to the recovery of the global economy following the COVID-19 pandemic. The primary model under consideration involves running the CBPR system in a separate forum outside of APEC and opening it up for participation by all qualifying countries. Indeed, the APEC Privacy Framework itself encourages the creation of globally interoperable privacy frameworks.

17. Can companies based in non-APEC economies obtain CBPR and PRP certification?

Not currently. See above answer. However, any of their corporate affiliates based in an APEC economy that participates in the CBPR may obtain certification for itself in that economy (but not for any of its other affiliates).

18. Could there be interoperability between the CBPR and EU mechanisms like Binding Corporate Rules (BCR) and GDPR certifications?

Yes. From 2013-2014, APEC and the EU's Article 29 Working Party (now the European Data Protection Board (EDPB)) mapped the substantive requirements of EU Binding Corporate Rules (BCR) and the CBPR and developed a common referential to identify substantive overlap and gaps between the two accountability and transfer mechanisms [6]. The next stage of this collaboration explored the possibility of interoperability tools that would allow companies that already were certified/approved in one system to get credit for compliance with overlapping requirements when seeking approval in the other system (to avoid duplicative approval and certification processes). However, this work was placed on hold due to other developments, such as the GDPR. In principle, this interoperability work could continue. As to interoperability between the CBPR and GDPR certifications, it would be possible to create interoperability, especially if the EU developed programmatic GDPR certifications that enabled certification of entire privacy programs. To date, no such GDPR certifications have been developed.

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

19. Where can I find more information?

At the official website for the CBPR and PRP systems: www.cbprs.org

If you would like to discuss this Q&A in more detail, please contact Markus Heyder, mheyder@huntonAK.com or Sam Grogan, sgrogan@huntonAK.com.

CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/.

References

[1] APEC CBPR, available at https://cbprs.blob.core.windows.net/files/CBPR%20Policies,%20Rules%20and%20Guidelines%20Revised%20For%20Posting%203-16.pdf.

[2] APEC PRP, available at https://cbprs.blob.core.windows.net/files/PRP%20Policies%20Rules%20and%20Guidelines%20Revised%20For%20Posting%203-16.pdf.

[3] The APEC Privacy Framework was developed by the 21 APEC member economies and was initially finalized in 2005. It includes nine Privacy Principles which the CBPR operationalize. See APEC Privacy Framework, available at https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf. Portions of the Framework were updated in 2015 and draw upon concepts introduced into the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980, updated in 2013) with due consideration for the different legal features and context of the APEC region https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).

[4] Existing Accountability Agents:

- TrustArc, United States, https://www.trustarc.com/products/apec-certification/;
- Schellman, United States, https://www.schellman.com/apec;
- NCC Group, United States, https://www.nccgroup.trust/us/;
- HITRUST, United States, https://hitrustalliance.net/apec/;
- JIPDEC, Japan, https://english.jipdec.or.jp/protection_org/cbpr/about.html;
- Korea Internet & Security Agency, South Korea, https://www.kisa.or.kr/eng/main.jsp;
- Infocomm Media Development Authority, Singpaore, https://www.imda.gov.sg/programme-listing/Cross-Border-Privacy-Rules-Certification.
- As further accountability agents are added, they will be listed at http://cbprs.org/business/.

[5] 26 participating PEAs:

US – Federal Trade Commission;
Japan – Personal Information Protection Commission
Australia – The Office of the Australian Information Commissioner (OAIC)
Australia (Victoria) – Office of the Victorian Information Commissioner, Privacy and Data Protection
New Zealand – The New Zealand Office of the Privacy Commissioner (NZOPC)
Hong Kong, China – The Office of the Privacy Commissioner for Personal Data, Hong Kong, China (PCPD)
Canada – The Office of the Privacy Commissioner of Canada (OPC)
Korea – Ministry of Interior – Korea (MOI)
Korea – Korean Communications Commission (KCC)
Singapore – Personal Information Protection Commission
Philippines – National Privacy Commission (NPC)
Chinese Taipei – Ministry of the Interior, Ministry of Foreign Affairs, Ministry of Education, Ministry of Justice, Ministry of Economic Affairs, Ministry of Transportation and Communications, Ministry of Labor, Council of Agriculture, Ministry of Health and Welfare, Ministry of Culture, Ministry of Science and Technology, Financial Supervisory Commission, Public Construction Commission, Fair Trade Commission, National Communications Commission

[6] See Article 29 Working Party Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents, adopted on 27 February 2014, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf.