

APEC's Cross-Border Privacy Rules System: Privacy Protection for the Asia-Pacific and Beyond

October 2017

Most consideration of international privacy rules focuses on the U.S.-EU Privacy Shield and the EU's General Data Protection Regulation (GDPR). Often overshadowed is the fact that there is also a system of privacy rules for the much more economically dynamic Asia-Pacific region. As this system expands, the benefits for companies certified under the system will likewise grow.

The CBPR System

The Cross-Border Privacy Rules (CBPR) system was established under the auspices of the Asia-Pacific Economic Cooperation (APEC), which consists of 21 member economies along the Pacific Rim. Members range from the United States and Chile to Singapore and Russia, and represent about 54% of the global economy. APEC generally operates on a consensus-based approach to develop voluntary standards. Despite this approach, APEC members often adopt APEC standards as binding, and APEC standards are frequently the foundation for later established global standards.

APEC members established the CBPR system in 2011 with the goal of establishing meaningful protection for the privacy and security of personal information, while ensuring the free flow of personal information across borders. The CBPR system does this by requiring APEC members wanting to join to: 1) demonstrate that the CBPR system's principles are enforceable under national law; 2) identify the domestic authority that can enforce the CBPR system; and 3) identify an APEC-recognized third-party certifying organization. Once an APEC member joins the CBPR system, that APEC member's companies can

Practice Areas

Privacy, Cyber & Data Governance

participate in the CBPR system by having their privacy policies and practices reviewed and certified by the third-party certifying organization as meeting the CBPR system's requirements. Once a company is certified, the CBPR becomes enforceable against that company. Thus, the CBPR system is similar to the U.S.-EU Privacy Shield by providing for self-assessment, compliance review, recognition and enforcement.

The CBPR system does not replace national law, nor does it require an APEC member to recognize another member's privacy system as adequate based on the other member having joined the CBPR system. Instead, it provides harmonization in privacy protection systems and establishes minimum standards for privacy protections. The CBPR system bridges across differences between domestic privacy approaches by applying commonly agreed-upon principles and rules. Having more harmonized privacy protection systems that meet minimum standards in turn helps facilitate data flows between CBPR members. Companies can also market certification under the CBPR system to customers and business partners as an indicator of reliability and compliance.

Status and Prospects

So far, the United States, Canada, Mexico and Japan have joined the CBPR system. South Korea was recently formally approved to join, and Singapore have submitted an application. The Philippines, Thailand, Vietnam, Thailand, Australia, Taiwan and Hong Kong have also expressed interest in participating. Thus, while the CBPR system may have started slowly, it is moving toward a critical mass of APEC members. Commerce Secretary Wilbur Ross stated on October 17 that he is seeking to expand the CBPR system to more APEC members. U.S. companies certified under CBPR include Apple, HP, IBM, Cisco Systems, Lynda.com, Merck, and Box.

The benefits of the CBPR system are expected to further expand. First, though not required to, APEC members may begin to recognize companies' certification under the CBPR system as meeting that member's domestic privacy requirements. This already happened when Japan recently amended its Protection of Personal Information Act (PPIA) to allow data transfers out of Japan to companies certified under the CBPR system. This is particularly important for U.S. companies given that the Japanese government recently indicated that it does not plan to give the United States a blanket designation of providing adequate data protection.

Second, the CBPR system could become the basis for a global privacy protection system, or at least become interoperable with other systems. There is an ongoing effort between APEC and the EU to explore the interoperability between the CBPR system and the EU's GDPR. A meeting between APEC and EU working groups was held last August, and the agreed goal is to develop a joint work plan by 2018. Commerce Secretary Ross also recently said that Commerce is exploring how to make the CBPR system and the EU's regime compatible.