

Fact Sheet

Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) Systems Certification

Background

The APEC Cross Border Privacy Rules (“**CBPR**”) and Privacy Recognition for Processors (“**PRP**”) Systems¹ are accountability-based and enforceable certifications developed by APEC economies to build consumer, business and regulator trust in cross border flows of personal data.

The APEC CBPR and PRP Systems establish a harmonised set of data protection standards consistent with the APEC Privacy Framework². The Systems bridge jurisdictional data protection laws and enable trusted data transfers, while ensuring high standards of data protection policies. Together, they enable certified organisations to transact with other certified organisations across APEC seamlessly, thus reducing barriers to global trade and the flow of data.

The Infocomm Media Development Authority (“**IMDA**”) has been appointed Singapore’s Accountability Agent (“**AA**”). Organisations which wish to be certified may do so through IMDA with immediate effect.

As the AA, IMDA will ensure that the data protection policies and practices of participating organisations comply with the APEC CBPR and PRP Systems through independent third-party assessors before certifying them. Certified organisations can display the APEC CBPR and PRP logos (below) on their corporate materials, and the certification is valid for one year.



APEC Cross Border Privacy Rules (CBPR)²



APEC Privacy Recognition for Processors (PRP)³


Benefits of APEC CBPR and PRP Systems

The APEC CBPR and PRP Systems benefit organisations by:

- **Building trust and confidence** in an organisation through the demonstration of a high-standard commitment to data protection to business counterparts and customers;
- **Reducing costs and time** with a single and consistent set of data protection standards that facilitates trusted international data flows, and reducing compliance costs;
- **Providing internal assurance** to the organisation by validating its data protection standards; and,

¹ CBPR systems apply to data controllers – companies which control the collection, holding, processing or use of data. PRP systems apply to data processors – companies which manage data on behalf of other companies at the latter’s instruction

² The APEC Privacy Framework was endorsed by 21 APEC economies in 2011 to promote accountable and responsible transfers of personal information between APEC economies.

³ “APEC”, “Cross Border Privacy Rules”, “CBPR”, “Privacy Recognition for Processors” and “PRP” are marks which belong to the Asia-Pacific Economic Cooperation. All other marks used, including but not limited to “”, belong to IMDA.

- **Demonstrate good faith compliance** to enforcement authorities.

Organisations such as Accenture, CrimsonLogic, Salesforce and TRS Forensics have recognised the value of CBPR certification and have indicated their interest to be certified.

Certification Costs and Process

The certification involves two fees:

- (1) Application fee of \$535 (inclusive of GST) payable to IMDA
 - Waived for SMEs until 30 June 2020
- (2) Assessment fee payable to the third-party Assessment Body
 - Ranges between \$1,000 to \$8,000 depending on the size of the organisation and the scope of the assessment required, plus prevailing GST

To encourage Singapore-based organisations to apply for the CBPR and PRP Systems, Enterprise Singapore offers support to eligible organisations to defray costs for the assessment fee and consulting services.

In addition, IMDA is implementing an integrated application process for organisations which wish to apply for both Singapore's Data Protection Trustmark ("**DPTM**") certification and the APEC CBPR and PRP certifications at the same time. As the DPTM includes elements of both CBPR and PRP, the assessment process will be streamlined if done concurrently. Organisations which have already been DPTM-certified may also find it easier to attain CBPR and/or PRP certification, as they have already demonstrated that they have a robust data governance regime in place.

For more information, please visit www.imda.gov.sg/dpcertifications.

ISSUED BY THE INFOCOMM MEDIA DEVELOPMENT AUTHORITY, SINGAPORE

About Infocomm Media Development Authority (IMDA)

The Infocomm Media Development Authority (IMDA) leads Singapore's digital transformation with infocomm media. To do this, IMDA will develop a dynamic digital economy and a cohesive digital society, driven by an exceptional infocomm media (ICM) ecosystem – by developing talent, strengthening business capabilities, and enhancing Singapore's ICM infrastructure. IMDA also regulates the telecommunications and media sectors to safeguard consumer interests while fostering a pro-business environment, and enhances Singapore's data protection regime through the Personal Data Protection Commission. For more news and information, visit www.imda.gov.sg or follow IMDA on Facebook IMDAsg and Twitter @IMDAsg.

For media clarifications, please contact:

Eugene NEUBRONNER (Mr)
Manager, Communications and Marketing
DID: (65) 6211 1182
Email: eugene_neubronner@imda.gov.sg

CHUA Hian Hou (Mr)
Deputy Director, Communications and Marketing
DID: (65) 6202 4956
Email: chua_hian_hou@imda.gov.sg