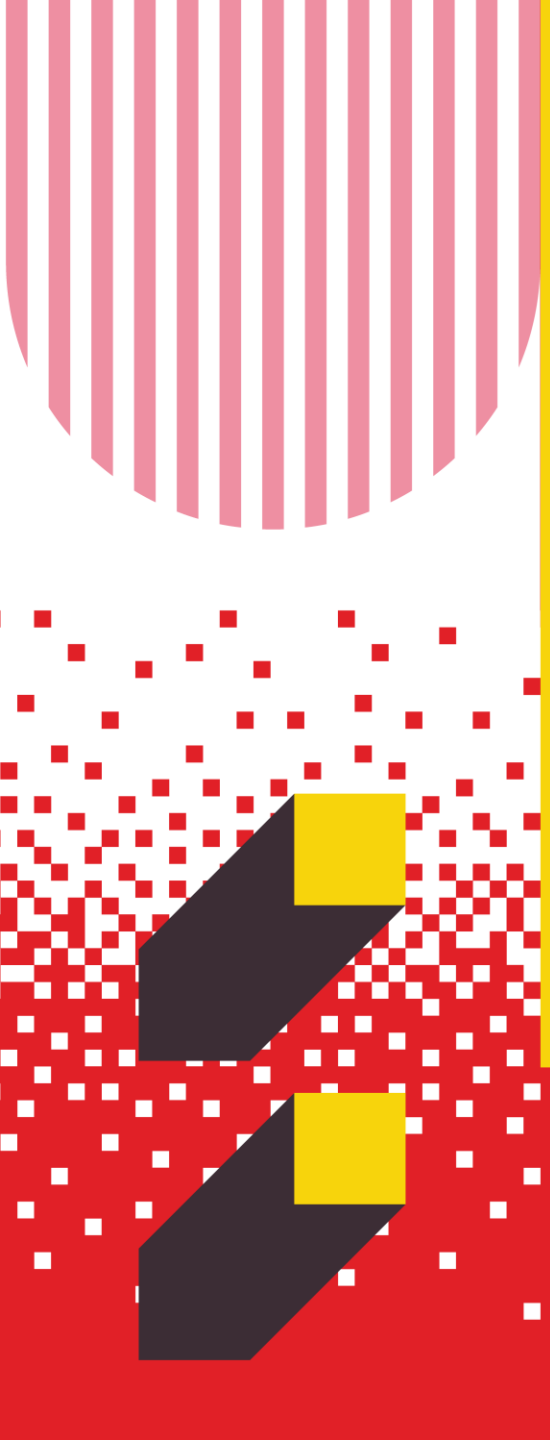




IAPP ASIA FORUM 2026

Privacy | AI governance | Cybersecurity law

Training 21 July

Conference 22-23 July | **SINGAPORE**

#IAPPForum26

WELCOME AND INTRODUCTIONS



Evelyn Goh, Director, International Relations, Policy & Strategy
Infocomm Media Development Authority (IMDA)



Eduardo Ustaran, AIGP, CIPP/E,
Partner, Hogan Lovells
Cadwalader



Justin B. Weiss, CIPP/A, CIPP/E,
CIPP/US, CIPM, FIP, Crowell Global
Advisors Senior Director, Senior
Counsel, Crowell & Moring

#IAPPForum26



Global Trends in Data Transfers

From Sovereignty to
Cross-Border Cooperation



#IAPPForum26

An evolutionary approach to data transfers

1. THE PRE-SNOWDEN YEARS (1995 – 2014)

- Focus on protection by the importer
- The birth of standard contractual clauses
- The emergence of BCR and CBPR

2. THE SCHREMS YEARS (2015 – 2020)

- Focus on government access to data
- *Safe Harbor* and *Privacy Shield* challenged
- The strengthening of standard contractual clauses

3. THE ERA OF DIGITAL SOVEREIGNTY (2021...)

- National security as reason for restrictions
- Zero-risk regulatory approaches
- New focus on data transfers to China

A pragmatic strategy in action

01

**Realistic
approach to
data
localisation**

02

**Demonstrable
confidence in
the level of
protection
afforded to
the data**

03

**Understanding
of the impact of
the third
country's data
access laws**

04

**Transparency
about the
destination of
international
data transfers**

05

**Perseverance
in adopting
defensible
mechanisms
to legitimise
data transfers**



#IAPPForum26

The U.S. policy lens on data sovereignty

In February '26, Reuters reported that U.S. Secretary of State Marco Rubio had issued a cable to all U.S. diplomats addressing digital sovereignty and related policy concerns:

“ the U.S. strongly supports cross-border data flows that promote growth and innovation while protecting privacy, safety, and free expression and stands ready to partner with countries that share those goal... . We seek to counter unnecessarily burdensome regulations, such as data localization mandates.”



A focus on trade commitments

- Both the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Regional Comprehensive Economic Partnership (RCEP) contained language relevant to data localization, e.g.,

CPTPP Article 14.11, Paragraph 2: "Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person."

- Recognizes exceptions for "legitimate public policy objectives," but subjects any such measure to a necessity test and prohibits arbitrary or unjustifiable discrimination or a disguised restriction on trade. RCEP Article 12.14 contains parallel commitments, binding Malaysia alongside 14 other Asia-Pacific nations.
- While the US withdrew from the CPTPP in 2017, such language aligns to the way that the U.S. administration appears to construe most data localization efforts, in particular in relation to industrial policy and the availability of U.S. AI tech stack.



U.S. National Security

Protecting Americans' Data from Foreign Adversaries Act (PADFAA)

PADFAA restricts U.S. data brokers from transferring Americans' sensitive personal data to foreign adversaries. The law focuses on limiting commercial access to categories of sensitive data—including precise geolocation, health, financial, biometric, and other personally identifiable information—to reduce national security risks. PADFAA targets cross-border data transactions with designated foreign adversaries and is currently in effect and being enforced.



While the TikTok divestiture is often cited as an example of U.S. efforts to address foreign adversary access to Americans' data, it was implemented under the **Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACAA)**, not PADFAA.



Executive Order 14117: Preventing Access to Americans' Bulk Sensitive Personal Data

Establishes a framework to restrict or prohibit certain transactions that could provide countries of concern with access to U.S. government-related data or bulk sensitive personal data. The DOJ's implementing regulations identify covered data categories and transactions, while providing exemptions for activities such as many commercial operations, financial services, and research under specified conditions.



U.S. approaches to Interoperability



Digital Economy Steering Group Data Privacy Subgroup (DPS)

- AIMP: APEC Project Database – the U.S., along with co-sponsoring economies Australia, Chile, Japan and Singapore, have undertaken research supporting *Information Sharing on Legal and Regulatory Interoperability for Privacy Protections in APEC*, recognizing the proliferation and diversity of data protection regimes across APEC member economies.
 - Considers, e.g. scope of applicability, legal bases, security (including breach notifications).
- Enforcement capabilities in data protection regimes
 - Trump v. Slaughter U.S. Supreme Court decision reopens focus on the criteria for independence in the trans-Atlantic context. EU and Convention 108 standard for independence of data protection authorities do not map seamlessly to all foreign government structures.
 - Public sector cooperation, including in law enforcement regimes, can underpin trusted structures
 - From convergence/divergence of data protection regimes to mutual respect, cooperation and digital trade

#IAPPForum26

Global Trends in Data Transfers: From Sovereignty to Cross-Border Cooperation

An update on the Global CBPR Framework



#IAPPForum26

Global Cross-Border Privacy Rules & Privacy Recognition For Processors

First developed by APEC Economies to bridge different privacy laws, reduce barriers and to build consumer, business and regulator trust in cross border flows of personal information, brought over to the global stage

GLOBAL CROSS-BORDER PRIVACY RULES (CBPR)

- A voluntary, accountability-based system that facilitates **trusted data flow** among participating jurisdictions
- Designed for **Data Controllers (DCs) to demonstrate accountability in data protection**
- Based on 9 principles of the Global CBPR Privacy Framework



PRIVACY RECOGNITION FOR PROCESSORS (PRP)

- A recognition system for **Data Processors** (Data Intermediaries) to demonstrate their ability in complying with relevant privacy obligations
- Controllers remain responsible for activities of their processors
- Based on 2 principles of the Global CBPR Privacy Framework

For more details: [Cross-Border Privacy Rules & Privacy Recognition for Processors](#)

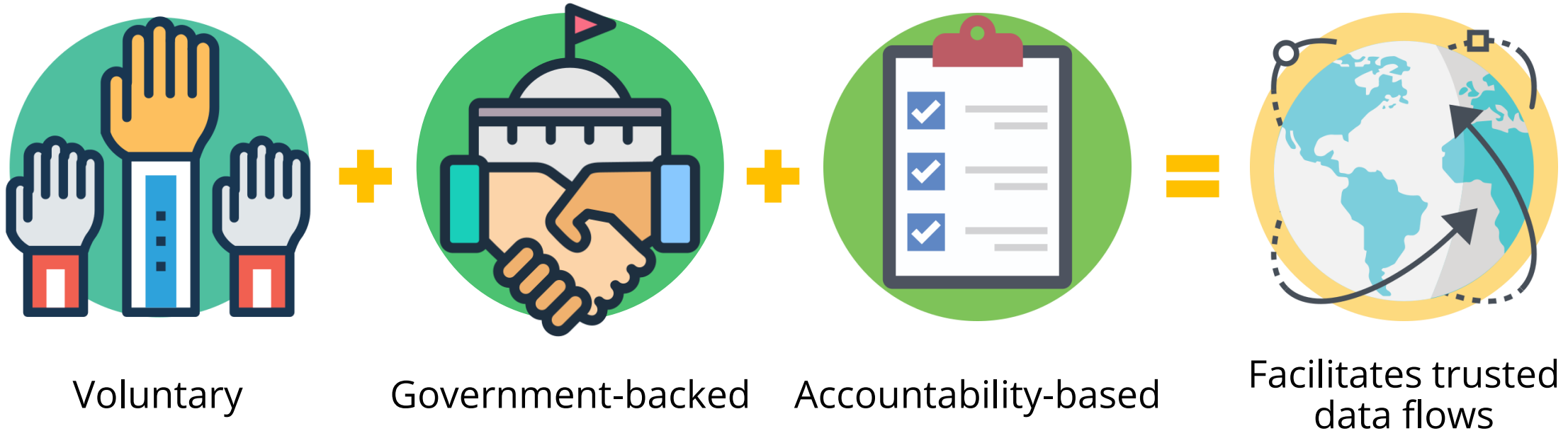
#IAPPForum26

Global Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) Systems

- **APEC CBPR & PRP** - Launched in 2011 by 21 APEC economies
- **Global CBPR** - Established in April 2022 to expand beyond APEC
- Global CBPR and PRP certifications launched on 2 June 2025 with about 100 certified companies covering over 2000 entities.
- ASEAN Digital Ministers endorsed the Operational Framework for Global CBPR and Global PRP in January 2025
- As of 2 March 2026, Singapore's Personal Data Protection Regulations amended to recognise both the Global CBPR and the Global Privacy Recognition for Processors (PRP) Systems.



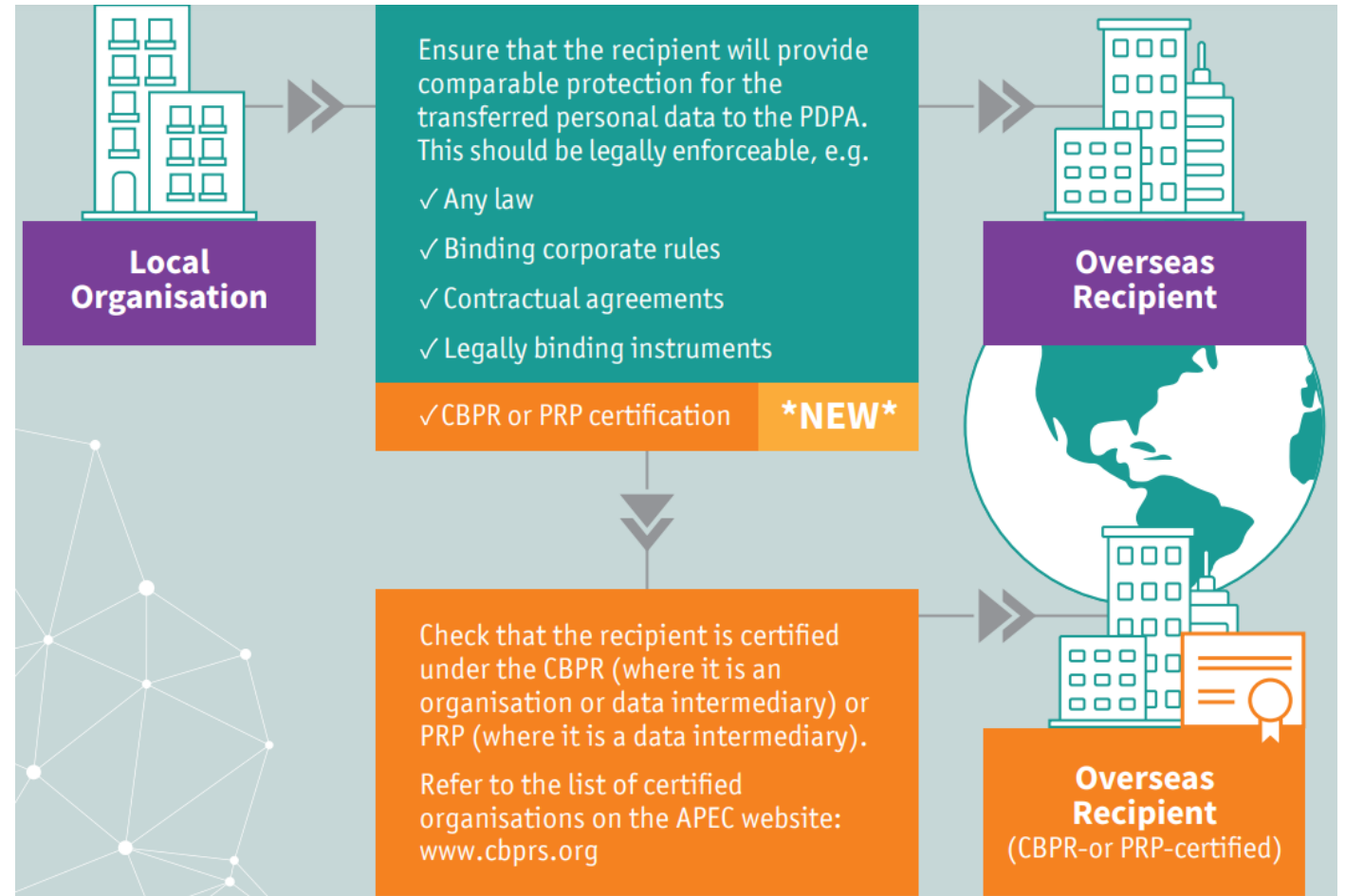
Global Cross-Border Privacy Rules & Privacy Recognition For Processors



#IAPPForum26

Global CBPR & PRP as Transfer Tools

- An overseas recipient that is **Global CBPR - or PRP-certified** is considered legally bound to provide comparable protection for the transferred personal data to the PDPA.
- Organisations in Singapore can transfer personal data to the overseas recipient without meeting additional requirements.
- PDPC has published **sample clause** for organisations to include in their contracts with the Global CBPR- or PRP-certified overseas recipient.



Global CBPR Privacy Principles



- Based on the core principles of the OECD's **Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data**.
- Basis for the Global CBPR and Global PRP Program Requirements, which organisations must implement to be certified.
- **Effective 1 April 2027: (1) Preventing Harm** has been introduced as a new programme requirement, and amendments have also been made to **(5) Choice** and **(9) Accountability**.
 - All new certifications and recertifications must meet these updated requirements.

The Global CBPR Certification will expand from 50 Programme Requirements (PRs) to 57 PRs

- Global CBPR Program Requirements adopted April 2024
 - Based on APEC CBPR Program Requirements established in 2011
- Members endorsed updates in September 2025
- Updates published on 23 March 2026
 - To be in force 1 April 2027

Sensitive Data	Direct Marketing Choice
Breach Notification to Individuals	Privacy Personnel
Risk Assessment	Withdrawal of Consent
Records of Processing and Consent	Children's Data



Global CBPR Members and Associates

Global CBPR Forum Members

- Australia
- Canada
- Dubai International Financial Centre
- Japan
- Republic of Korea
- Mexico
- Philippines
- Singapore
- Chinese-Taipei
- United States

Global CBPR Forum Associates

- Bermuda
- Mauritius
- Nigeria
- United Kingdom

Jurisdictions in discussion with the Global CBPR Forum:

Malaysia, Thailand, Brunei, Indonesia, Vietnam, Bangladesh, Nepal, Sri Lanka, South Africa, Egypt, Qatar, Argentina, Peru, Ecuador, Chile and more....



Global Cooperation Arrangement for Privacy Enforcement (Global CAPE)

- Multilateral Mechanism for Data Protection Authorities to cooperate in cross-border data protection enforcement.
- **Facilitates:**
 - Information sharing among Privacy Enforcement Authorities (PEAs)
 - Mechanism for cross-border enforcement cooperation
- **All data protection authorities can join – no need to be a member of the Forum**
 - Global CAPE currently has 29 participants from 14 jurisdictions - Australia, Bermuda, Canada, Dubai International Financial Centre, Japan, Republic of Korea, Mexico, the Philippines, Singapore, South Africa, Thailand, Chinese-Taipei, the United Kingdom, the United States



Global CBPR-Recognised Accountability Agent (AA)

- AAs are independent organisations recognised by the GCBPR Forum, to assess whether companies meet the Global CBPR or Global PRP Program Requirements.
- **Key Criteria/Responsibilities:**
 - **Certify:** Evaluate a company's privacy governance, policies, and controls against Global CBPR requirements to grant Global CBPR or Global PRP certification to organisations.
 - **Monitor:** Conduct periodic reviews and recertifications to ensure continued compliance.
 - **Resolve Disputes:** Investigate complaints relating to certified organisations and coordinate with Privacy Enforcement Authorities where necessary.
- Apply to become a forum-recognised accountability agent:



Global CBPR Accountability Agents

United States

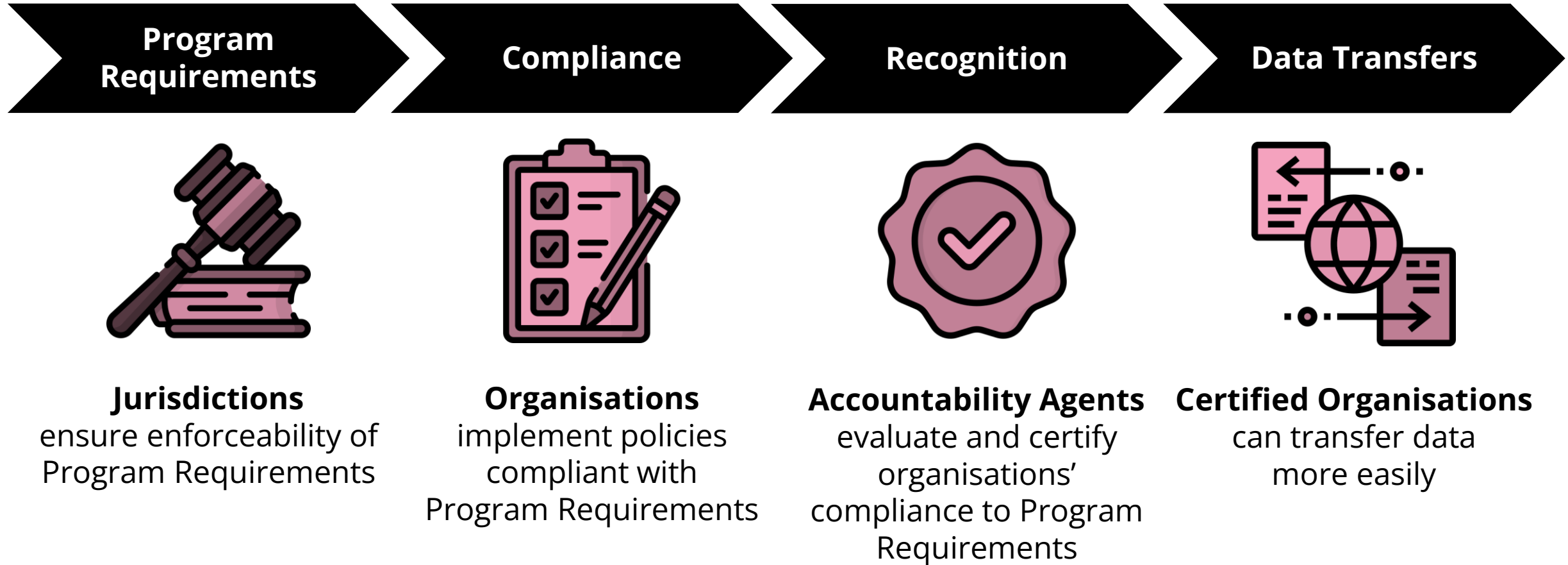


Chinese Taipei, Japan, Korea, Singapore,



There are currently **9** Accountability Agents from **5** jurisdictions.

How do the Systems work?



Global CBPR – Certification in Singapore



Online
Application



Perform Self-
Assessment



Appoint
Assessment
Body



Conduct
Assessment



Attain
Certification

1. BSI Singapore Pte Ltd
2. EPI Certification Pte Ltd
3. Guardian Independent Certification Pte Ltd
4. ISOCert Pte Ltd
5. Setsco Services Pte Ltd
6. SOCOTEC Certification Singapore Pte Ltd
7. TÜV SÜD PSB Pte Ltd



#IAPPForum26

Benefits of Participating in the Global CBPR

GOVERNMENTS

- Development of international standards
- Help jurisdictions develop data protection regimes
- Increase general compliance & trust
- Facilitate cross-border enforcement
- Efficiency gains

ORGANISATIONS

- Facilitate cross-border data transfers
- Reduce cost and time
- Enable compliance with domestic law and international standards
- Help SMEs develop data protection programs
- Demonstrate accountability
- Due diligence tool
- Mitigating factor in enforcement

CONSUMERS

- Enhanced protection of personal data
- Choice of trusted vendor
- Consumer-friendly complaint/dispute resolution handling

PROMOTE CONNECTIVITY, INNOVATION & TRUST
SUPPORT CONSUMER PROTECTION & TRADE

#IAPPForum26

Global CBPR and PRP Certified Organisations in Singapore



There are currently **138** organisations from **5** jurisdictions, covering more than **2000** entities on board and certified globally.

#IAPPForum26

Global CBPR Forum Annual Work Programme (2026–2027)



Goal 1: Expand Global CBPR & PRP Systems

- Implement the updated Global CBPR Program Requirements
- Support Members in establishing Accountability Agents and increasing certification uptake
- Increase the number of certified companies by 50%



Goal 2: Strengthen the Global CBPR Forum

- Expand participation through new Associates and Members
- Encourage wider participation in Global CAPE by Privacy Enforcement Authorities
- Multistakeholder workshops (Fall 2026 & Spring 2027)
- Enhance information sharing through website resources



Strategic Goal 3: Improve Forum Governance

- Review governance documents, procedures, and resources
- Implement improvements to strengthen accountability, efficiency, and effectiveness



#IAPPForum26

Global CBPR Website: Call for Blog Post Contribution



Global CBPR Forum welcomes blog post submissions from individuals who have relevant experience, expertise, or any meaningful contributions to relevant topics.

Submission and Review Process:

Submission and Initial Review*

Editorial Review and Feedback

Final Approval and Scheduling

Post-Publication Monitoring

*Contributors may submit their posts along with any required supporting materials to comms@globalcbpr.org via email

#IAPPForum26

RESOURCE LIST

- <https://www.globalcbpr.org/>



How Did Things Go? (We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Forum 2026**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!



#IAPPForum26