Centre for Information Policy Leadership (CIPL) and
Personal Data Protection Commission (PDPC) Joint Workshop on

# Roles of Certifications in Personal Data Protection

15 November 2018, Singapore

WIFI: IC@Ballroom
Password: itk00002

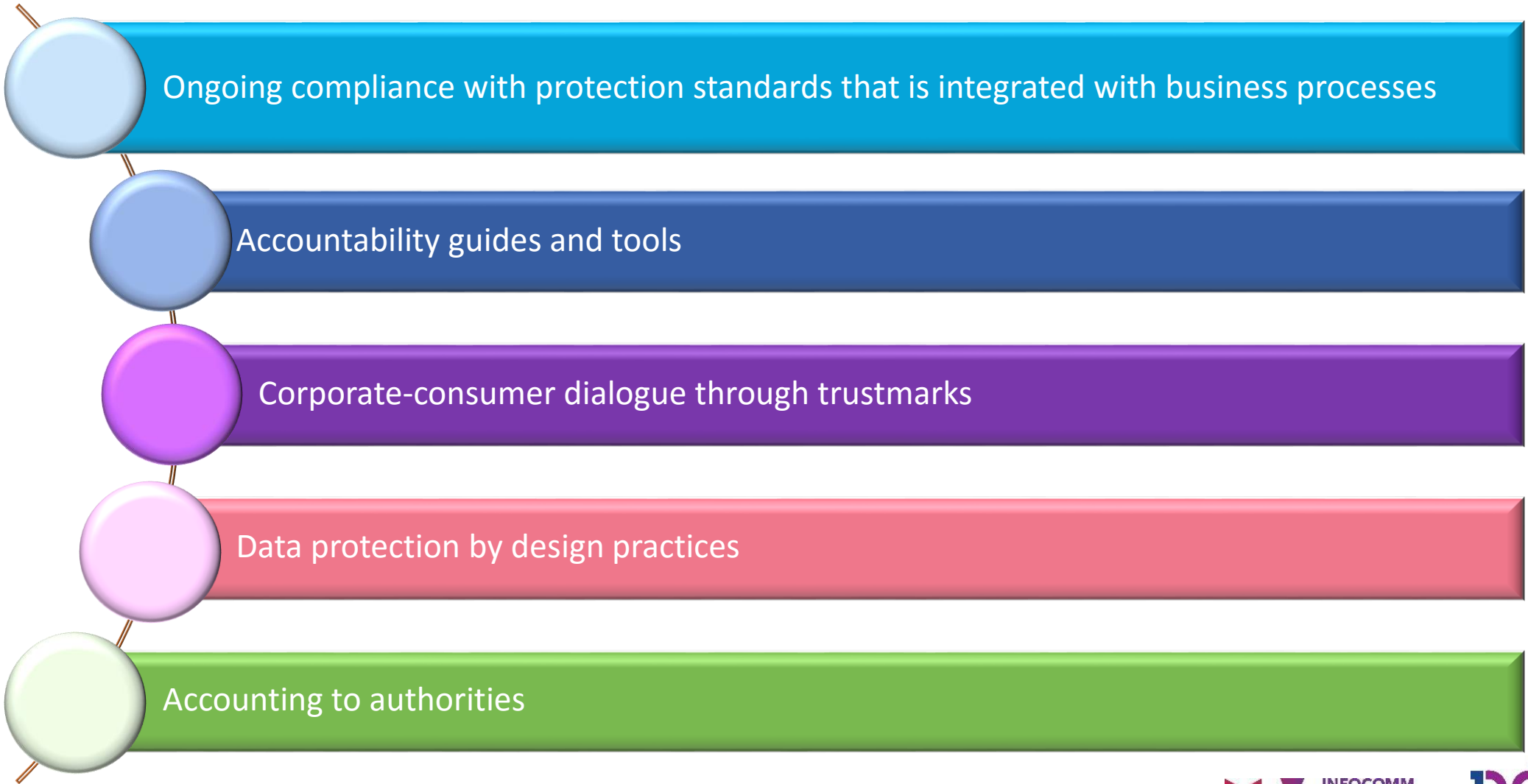
Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

pdpc
PERSONAL DATA PROTECTION COMMISSION SINGAPORE

# Opening Remarks

**YEONG ZEE KIN**
**Deputy Commissioner, PDPC**

# ACCOUNTABILITY EMPHASES




INFOCOMM MEDIA DEVELOPMENT AUTHORITY

pdpc SINGAPORE


*"While the PDPA will remain progressive, we cannot be solely reliant on laws. Organisations must also develop a culture of accountability to build consumer trust…*

*The DP Trustmark would be a **visible badge** of recognition for accountable and responsible data protection practices used by organisations, including appropriate data protection policies and practices, adequate measures to identify and address data protection risks, and a sound data breach management plan."*

Mr S Iswaran

Minister for Communications and Information

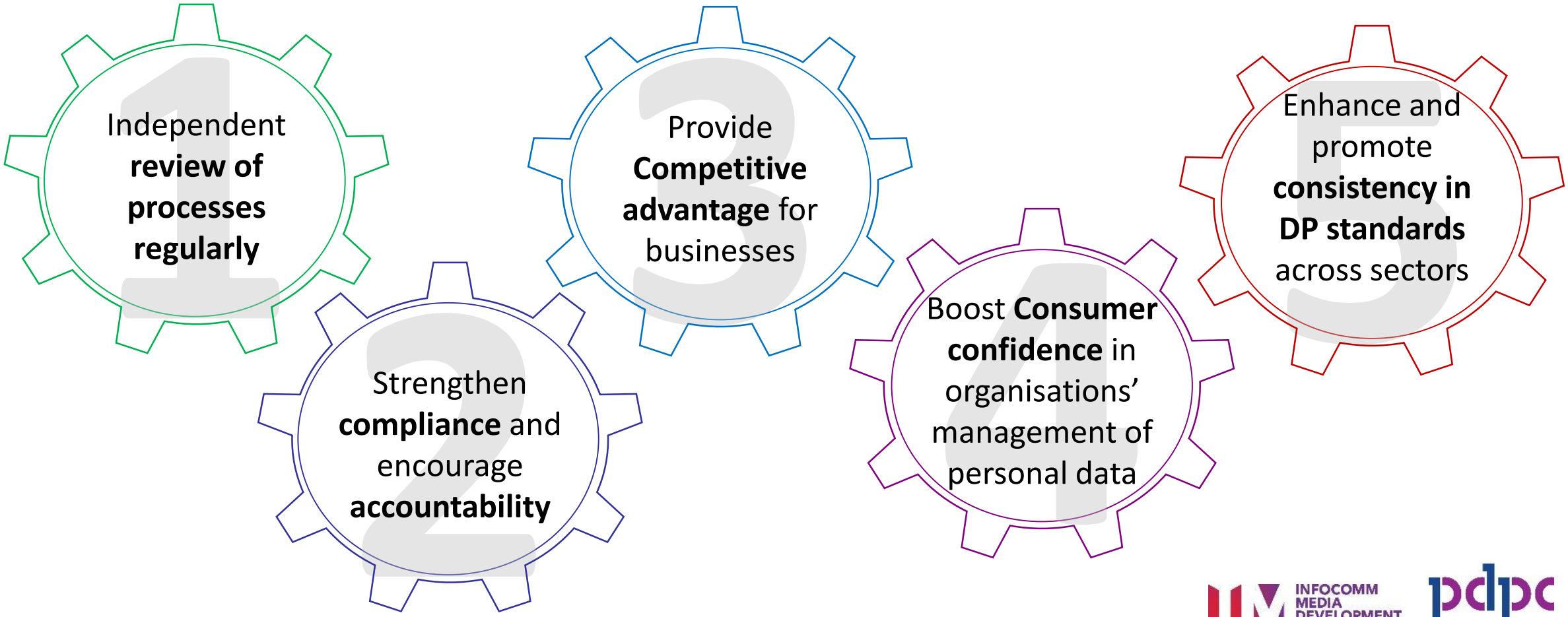
Personal Data Protection Seminar 2018

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

pdpc SINGAPORE

# DATA PROTECTION TRUSTMARK CERTIFICATION

**Establishing and recognising robust data governance standards to help organisations increase their competitive advantage and build trust with their clients**




INFOCOMM MEDIA DEVELOPMENT AUTHORITY

pdpc SINGAPORE

# DPTM CERTIFICATION STANDARD

**Singapore's PDPA DP Obligations**

- Consent
- Purpose Limitation
- Notification of Purpose
- Access
- Correction
- Accuracy
- Protection
- Retention Limitation
- Transfer Limitation

**International benchmark, best practices**

DP laws of other jurisdictions like Australia, Hong Kong, EU + international benchmarks like OECD Guidelines, APEC Privacy Framework (including CBPR, PRP)

**Principles for Singapore's DPTM Certification Framework**

- Governance and Transparency
- Management of Personal Data
- Care of Personal Data
- Individual's Rights

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

pdpc SINGAPORE

# RANGE OF POSSIBLE INCENTIVES UNDER THE DPTM FRAMEWORK

Recognition for cross-border transfer

Regulatory relief

Exemption applications

Recommended criteria for supply of goods/services to government

Participation in IMDA platforms

Adoption incentives for SMEs

Invitation / Recognition as PDPC's industry champions

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

pdpc SINGAPORE

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

pdpc
PERSONAL DATA PROTECTION COMMISSION SINGAPORE

# Thank You

# Opening Remarks

**BOJANA BELLAMY**
**President, CIPL**

# The Significant Role of Certifications

## Demonstrate accountability and compliance

- Enable organisations to achieve and demonstrate accountability and ensure local compliance

## Enable international data transfers

- Enable organisations to transfer data responsibly, safely and efficiently across borders

## Facilitate interoperability

- Organisations need to be able to leverage different certifications as they build their privacy program and certifications need to work with each other

# The Certifications Landscape in Europe and Asia

## Europe Post-GDPR

- EDPB draft guidance on certifications (May 2018)
- EDPB draft guidance on the accreditation of certification bodies under Regulation (February 2018)
- EU Commission study on certifications in progress

## APEC CBPR/PRP

- **Joined**: US, Canada, Mexico, Japan, South Korea and Singapore
- **Formally started process**: Taiwan and Australia
- **Filing application this year**: The Philippines
- **Considering joining**: Vietnam, Peru, Chile, Papua New Guinea, New Zealand

## National Certifications

- **Singapore Data Protection Trustmark**: Developed by PDPC and administered by IMDA. DPTM pilot concluded (September 2018)
- **Japan PrivacyMark**: Since 1998 and 15,969 certified entities

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

# CIPL Engagement on Certifications

**Engaged in APEC CBPR process and the work on interoperability between APEC and the EU**

**Active on GDPR issues relating to BCR, Certifications and Codes of Conduct**

**Involved in the Privacy Shield Review Process**

**Working on an interoperability report to demonstrate overlap between different accountability schemes, including certifications**

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

# Relevant CIPL Papers

1. CIPL White Paper on Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms (April 2017)

2. CIPL White Paper on Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy (September 2017)

3. CIPL Comments to WP29 Updated Working Documents Setting Up Tables for Binding Corporate Rules and Processor Binding Corporate Rules (January 2018)

4. CIPL Comments to WP29 Draft Guidelines on the accreditation of certification bodies (March 2018)

5. CIPL Comments to EDBP Draft Guidelines on certification and identifying certification criteria in accordance with articles 42 and 43 of the GDPR (July 2018)

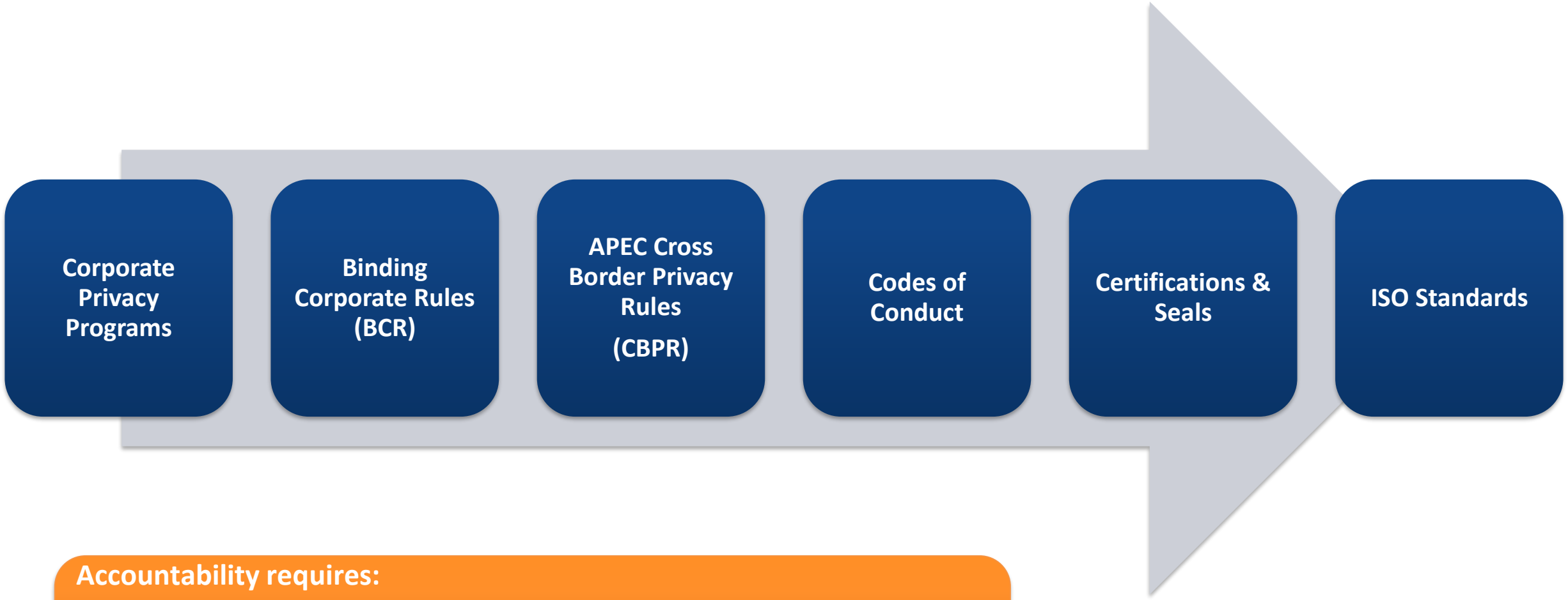
# Topic I: The Role of Certifications as Accountability and Compliance Tools

- **Jacobo Esquenazi, Global Privacy Strategist, HP, Inc.**
- **Yi Lin Seng, Senior Counsel, Mastercard**
- **Alex Li, Program Manager, Microsoft**
- **Darren Abernethy, Senior Counsel, TrustArc**
- **Eunice Toh, Executive Director, Tan Tock Seng Hospital Community Fund**

**Moderator: Bojana Bellamy, President, CIPL**

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

# Certifications Demonstrate Accountability and Local Compliance




**Accountability requires:**

- **Following substantive privacy rules**
- **Implementation infrastructure**
- **Verification**
- **Ability to demonstrate**

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

# Benefits of Certification

## Organisations

- Demonstrates accountability and compliance (internally and externally)
- Operationalises compliance
- Scalable for SMEs and start-ups
- B2B due diligence and risk management
- Enables cross-border data transfers
- Potentially expands organisations' geographic reach and coverage
- Potential mitigating factor in DPA oversight and enforcement actions

## Individuals

- Creates trust
- Provides greater transparency
- Provides assurance of effective privacy protection on the part of organisations

## DPAs

- Reduces oversight workload
- Enables more effective compliance on the ground
- Reduces complaint-handling obligations
- Increases transparency

# Privacy Certifications

What is the Value

Jacobo Esquenazi / November 15, 2018

**@jesquenazi**
**MX**

# Certifications Value to Companies

**Benchmarking**

**Data Transfers**


**Customer Demonstration**


Singapore


Germany


**Competitive Advantage**

# HP Certifications Timeline

2001 | 2011 | 2012 | 2015 | 2016 | 2018

U.S. • EU SAFEHARBOR

HPQ BCR-C

TRUSTe APEC Privacy Powered by TrustArc

HPQ CBPR

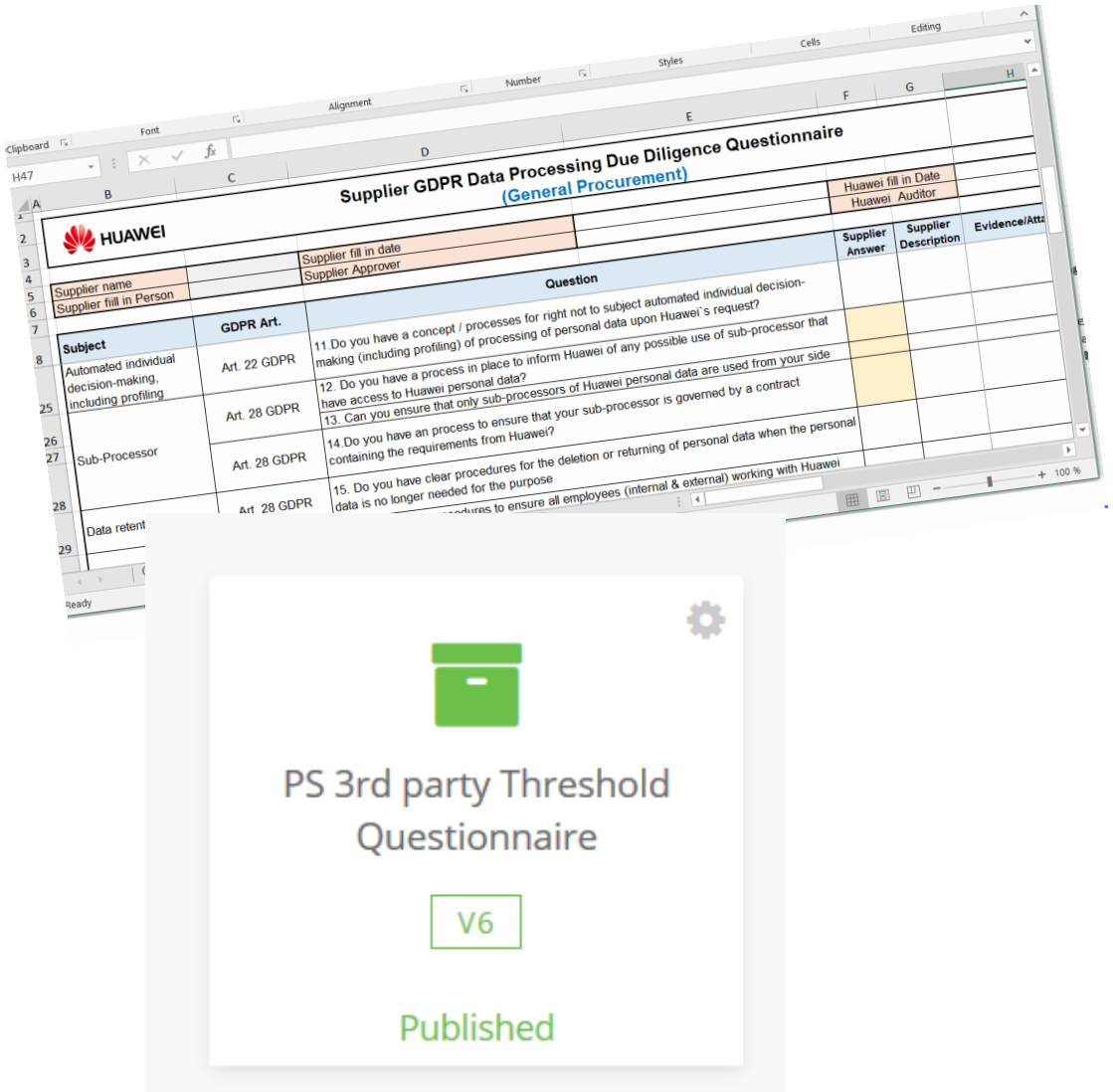
HP BCR-C

TRUSTe APEC Privacy Powered by TrustArc

HP CBPR

HP BCR-P

# Certifications as a Tool to Conduct Due Diligence




GDPR 28.5: Adherence of a processor to an approved code of conduct as referred to in Article 40 or **an approved certification** mechanism as referred to in Article 42 may be used as an element by which to **demonstrate sufficient guarantees** as referred to in paragraphs 1 and 4 of this Article.

# Interoperability – Why?


@jesquenaziM
X

Microsoft

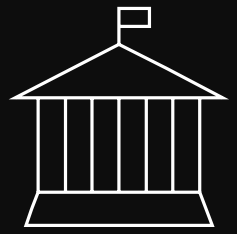
# The Role of Certifications as Accountability and Compliance Tools

Alex Li
Privacy and Regulatory Affairs

# Who is demanding privacy certification? Why?

**Consumers?**

- Very little evidence of consumer awareness, demand, or decision-making based on privacy certifications
- Trust is earned



**Regulators?**

- Certifications are voluntary
- Regulators should make certain that certifications are trustworthy, but they are not the audience

**B2B?**

- GDPR stipulates that controllers are responsible for the entire data processing supply chain
- Sometimes a contract or self attestation is enough
- Sometimes you need to “Trust, but verify”

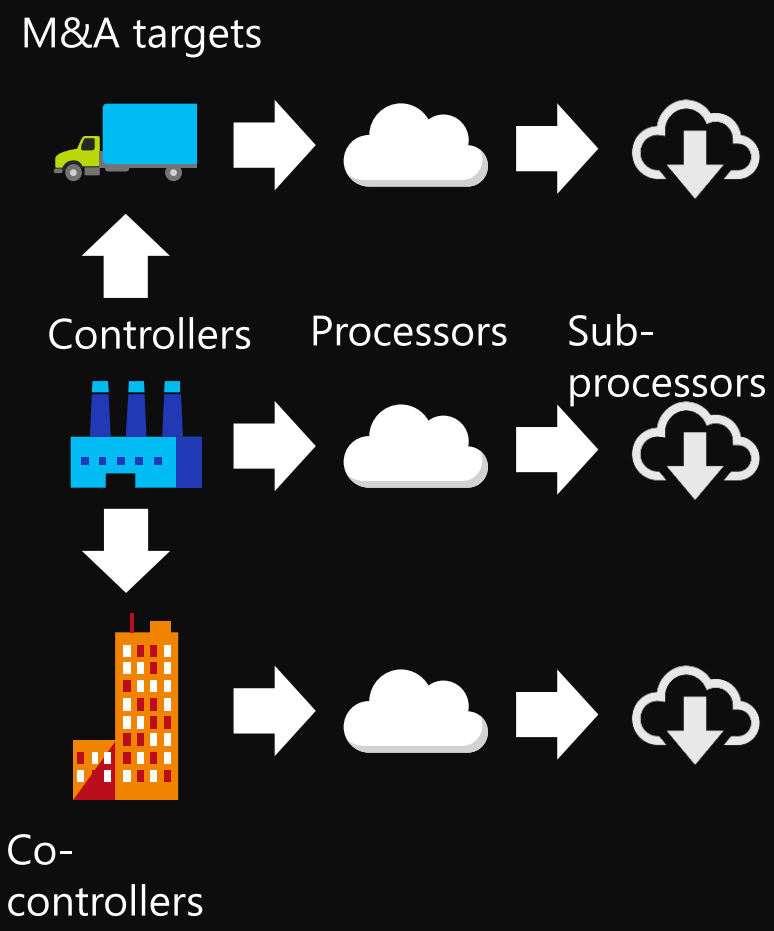
# GDPR stipulates compliance validation between various market actors

The need is most obvious through the data processing supply chain

but it is also important between co-controllers

and strategically important for M&A

Failure of one actor has potentially negative implication upward through the web of data processing supply chain



# What is Microsoft doing to encourage a scalable privacy certification market?

Encourage European DPAs, EDPB, and EC to establish a common certification scheme within EU

Invest in the development of ISO/IEC 27552, a privacy extension of ISO/IEC 27001, with European regulators

Map privacy regulations, including, GDPR, CaCPA, PDPA, and others, against ISO/IEC 27552

Model Microsoft's privacy management system, including its data processing supply chain, to align with ISO/IEC 27552

# The Role of Certifications as Accountability and Compliance Tools

## CIPL and Singapore PDPC Workshop

Darren Abernethy, Senior Counsel
TrustArc


**November 15, 2018**

# APEC CBPR & PRP Certifications – From an Accountability Agent's Perspective

- Six participating APEC CBPR System economies:  USA, Mexico, Canada, Singapore and the Republic of Korea, with more on the way

- The System aims to bridge aspects of differing privacy laws* within the APEC region to increase global trade and further the digital economy

- To become CBPR-certified, an org. must be subject to the laws of an APEC CBPR System participating economy, and undergo a thorough cert. process with an Accountability Agent in that economy annually

- AAs (e.g., TRUSTe in USA, JIPDEC in Japan) work collaboratively with companies, consumers and governments to ensure that cross-border data transfers meet the standards of the APEC Privacy Framework.  In the USA, the Federal Trade Commission is the enforcement authority

# Benefits of APEC CBPR & PRP Certifications

- A detailed privacy review, to confirm your org's APEC compliance work or remediate gaps previously unrecognized
- Proactively working with an approved AA to fix DP issues, rather than learning of issues belatedly from a regulator
  - **Note: National privacy laws must still be independently complied with*
- Ongoing monitoring, guidance and dispute resolution
- Having a searchable audit trail, a formal letter of attestation and public-facing use of the TRUSTe APEC Seal(s)


# Break

**Workshop will resume in 15 mins time**

WIFI: IC@Ballroom
Password: itk00002

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

pdpc
PERSONAL DATA PROTECTION COMMISSION SINGAPORE

# Session II: The Role of Certifications in Data Transfers and as a Mechanism for Global Interoperability

- **Florian Thoma,** Senior Director, Global Data Privacy, Accenture
- **Harvey Jang, Senior Director,** Global Data Protection & Privacy Counsel, Cisco
- **Toshiki Yano, Public Policy & Government Relations Counsel,** APAC Strategy & Operations, Google

**Moderator: Darren Abernethy, Senior Counsel, TrustArc**

# The Role of Certifications in Data Transfers and Global Interoperability

## CIPL and Singapore PDPC Workshop

Darren Abernethy, Senior Counsel
TrustArc


**November 15, 2018**

# Certifications as Cross-Border Transfer Mechanisms for Personal Data

- The idea behind data transfer certifications is to enable organizations to economically engage in cross-border data flows while ensuring protection against risks and harms to individuals
- "Interoperability" defined…i.e., leveraging privacy/DP compliance
- EU Binding Corporate Rules BCRs)– pre-GDPR only *intra*-company, post-GDPR broader ("enterprises engaged in a joint economic activity") but still being interpreted; potential cost/time/org size limitations
- GDPR Certifications – Current status and types, the BCR-CBPR "Referential," and comparison with adequacy decisions
- APEC CBPR & PRP Systems -- Enforceable, accountability-based mechanism for intra- *and* intercompany cross-border data transfers, approved by a 3rd party AA in the juris in which the organization is HQ'd

# Advantages of APEC CBPR & PRP Systems

- Symbol of trust for BoD and external consumers & partners, including in the business-to-business (B2B) context for risk mitigation and due dil.
- Scalability for both PI controllers (CBPR) and PI processors (PRP)—whether large MNCs or small and medium-sized enterprises (SMEs)
- Makes digestible and operational baseline elements of many privacy laws, bringing clarity by working with the AA as to what must be completed to meet APEC Privacy Framework compliance requirements
- Likely viewed favorably by regulators in participating economies
- APEC has seen critical growth in participating CBPR System economies, expansion of PRP, and participating organizations—as well as specific reference to the APEC Privacy Framework in national regulations + FTAs
- Centralization, built-out infrastructure, AA cooperation, & well-recognized

# Data Protection & Privacy @ Cisco

A Business Imperative

Harvey Jang
Senior Director
Global Data Protection & Privacy Counsel

November 2018

# Opportunity Landscape

Regulatory Compliance

Contractual Obligations

Customer & Market Expectations

Competitive Differentiation

## Strategic Considerations

# APEC Privacy Framework (2005, 2015)

1. Preventing Harm
2. Notice
3. Collection Limitation
4. Uses of Personal Information
5. Choice
6. Integrity of Personal Information
7. Security Safeguards
8. Access and Correction
9. Accountability


Asia-Pacific Economic Cooperation

#GPS18

# ASIA REGULATORY LANDSCAPE

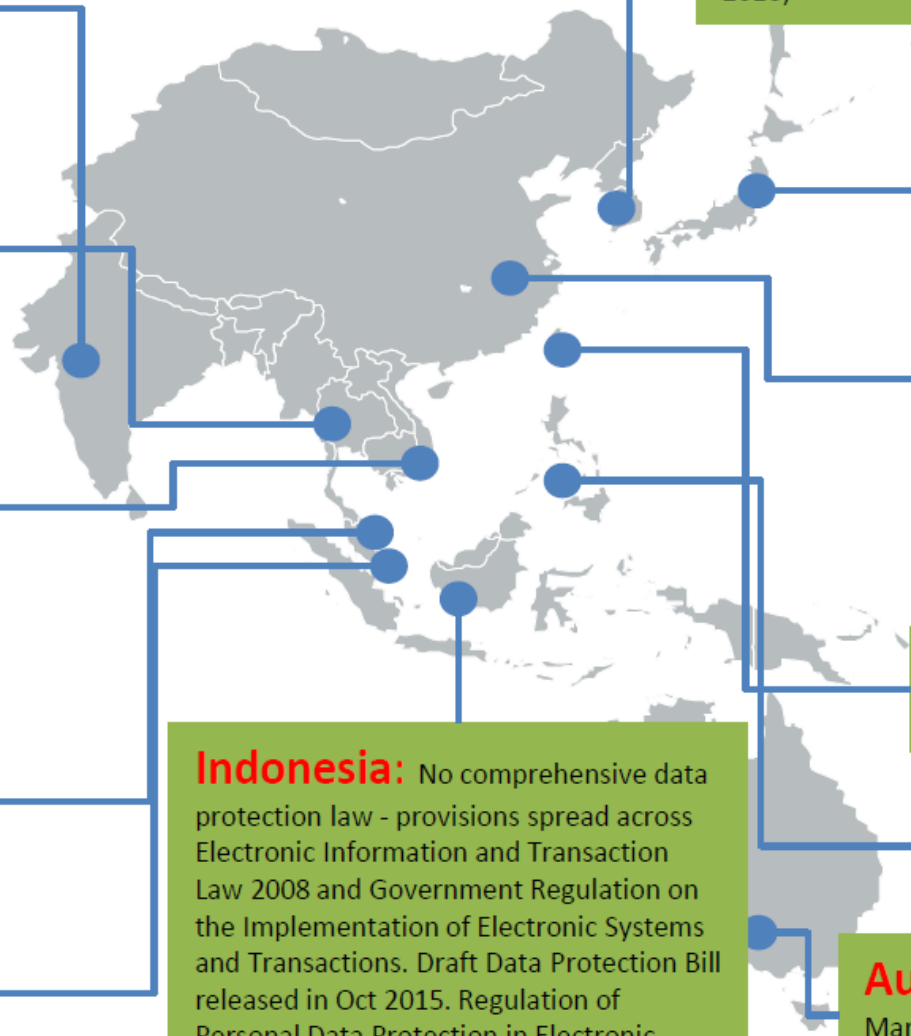
**India:** Right to Privacy Bill 2014 still under review. Currently provisions spread across the IT Act 2000;
the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) and Rules
and the IT (Intermediaries Guidelines) Rules 2011

**Thailand:** Draft Personal Data Protection Bill under review by National Legislative Assembly

**Vietnam:** No comprehensive data protection law - provisions spread across Civil Code, the IT Law, the Penal Code, the Telecommunications Law. The Cyber Information Security Law came into effect on July 1, 2016). On 6 June 2017, the first draft of the Law on Cybersecurity (Draft Law) was released for public consultation between 8 June and 8 August 2017

**Malaysia:** Personal Data Protection Act 2013 (Personal Data Protection Standards came into force on December 23, 2015 )

**Singapore:** Personal Data Protection Act 2012. Cybersecurity Bill passed by Parliament in Feb 2018



**Indonesia:** No comprehensive data protection law - provisions spread across Electronic Information and Transaction Law 2008 and Government Regulation on the Implementation of Electronic Systems and Transactions. Draft Data Protection Bill released in Oct 2015. Regulation of Personal Data Protection in Electronic Systems became effective on Dec 2016

**South Korea:** Personal Information Protection Act 2011 (amendments came into force Sept 2016)

**Japan:** Act on Protection of Personal Information 2013 (amendments came into force in May 30, 2017)

**China:** No comprehensive data protection law – provisions spread across NPC Decision on Strengthening the Protection of Network Information 2012; Amended PRC Consumer Law 2013; Provisions of the Supreme People's Court on Several Issues concerning the Application of the Rules regarding cases of the Infringement of Personal Rights over Information Networks 2014; Cybersecurity Law 2016

**Hong Kong:** Personal Data (Privacy) Ordinance (under review)

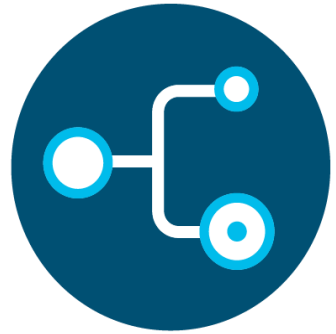
**Taiwan:** Personal Data Protection Act 2010 (amendments came into force March 2016)

**The Philippines:** Data Privacy Act 2012 (Implementing Rules and Regulations effective September 9, 2016)

**Australia:** Privacy Act 1988 (amendments in full effect on March 2014). Data breach notification scheme passed in Feb 2017 (in full effect Feb 2018)

# Cisco Data Protection & Privacy Program

Policies and Standards



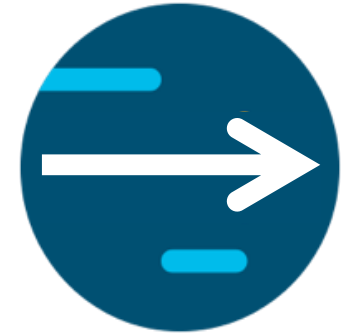
Identification and Classification

Data Risk and Organizational Maturity

Incident Response

Oversight and Enforcement

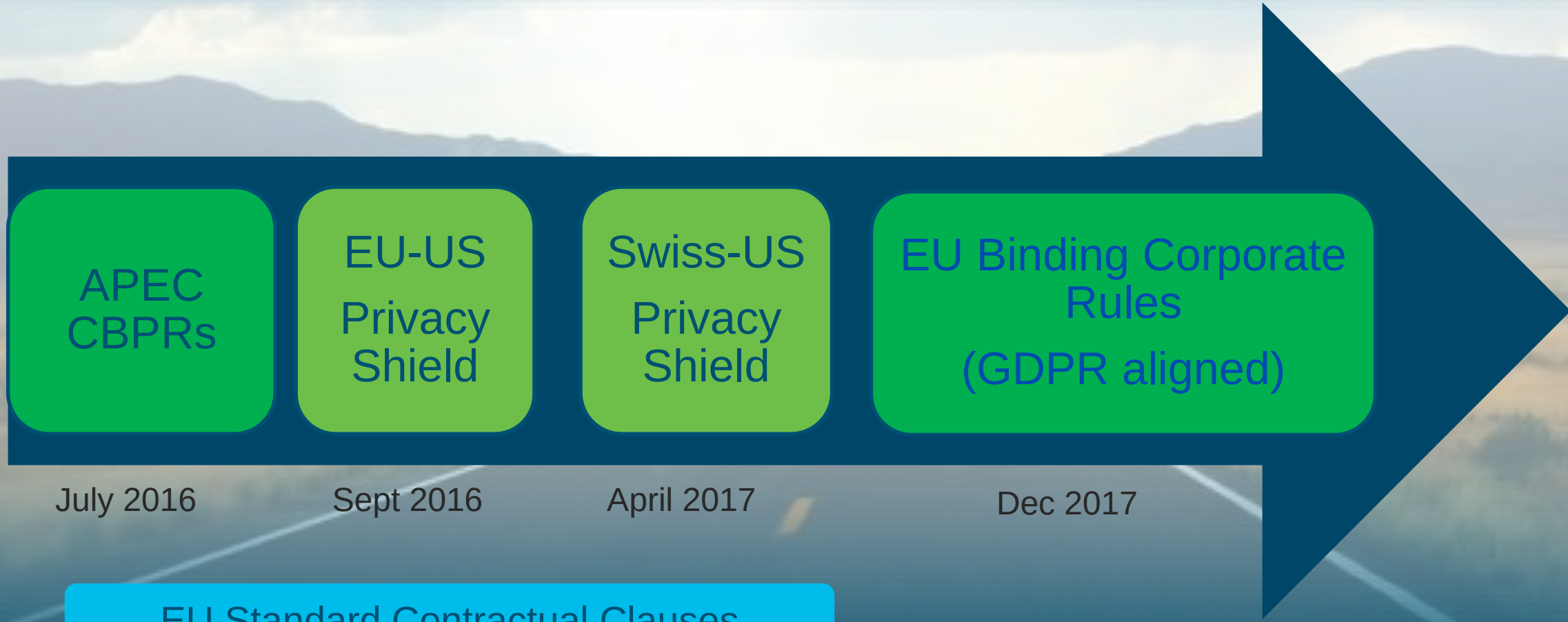
Awareness and Education



By Design

# Data Protection & Privacy Certifications

Transfer Mechanisms & Demonstrable Compliance




EU Standard Contractual Clauses

# Certification Benefits

- Demonstrable Compliance
- Proactive Accountability
- External Validation/Testing
- Global Interoperability and Consistency
- Mechanism for Cross-border Transfers
- Earn and Maintain Trust

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

# Closing Remarks

**Bojana Bellamy**
President, CIPL

# Contacts


**Bojana Bellamy**
President
Centre for Information Policy Leadership
BBellamy@huntonak.com

**Markus Heyder**
Vice President & Senior Policy Advisor
Centre for Information Policy Leadership
MHeyder@huntonak.com

**Nathalie Laneret**
Director of Privacy Policy
Centre for Information Policy Leadership
NLaneret@huntonak.com

**Sam Grogan**
Global Privacy Policy Analyst
Centre for Information Policy Leadership
SGrogan@huntonak.com


**Centre for Information Policy Leadership**
*www.informationpolicycentre.com*

**Hunton Andrews Kurth Privacy and Information Security Law Blog**
*www.huntonprivacyblog.com*

**FOLLOW US ON LINKEDIN**
linkedin.com/company/centre-for-information-policy-leadership

**FOLLOW US ON TWITTER**
@THE_CIPL