

Co-Hosted By



PRIVACY
SECURITY
SUMMIT

หัวข้อปาฐกถา

4: Regional Regulatory Framework RCEP & APEC

โดย

นาย วรรณวิทย์ อาชูปุตร

ที่ปรึกษาปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

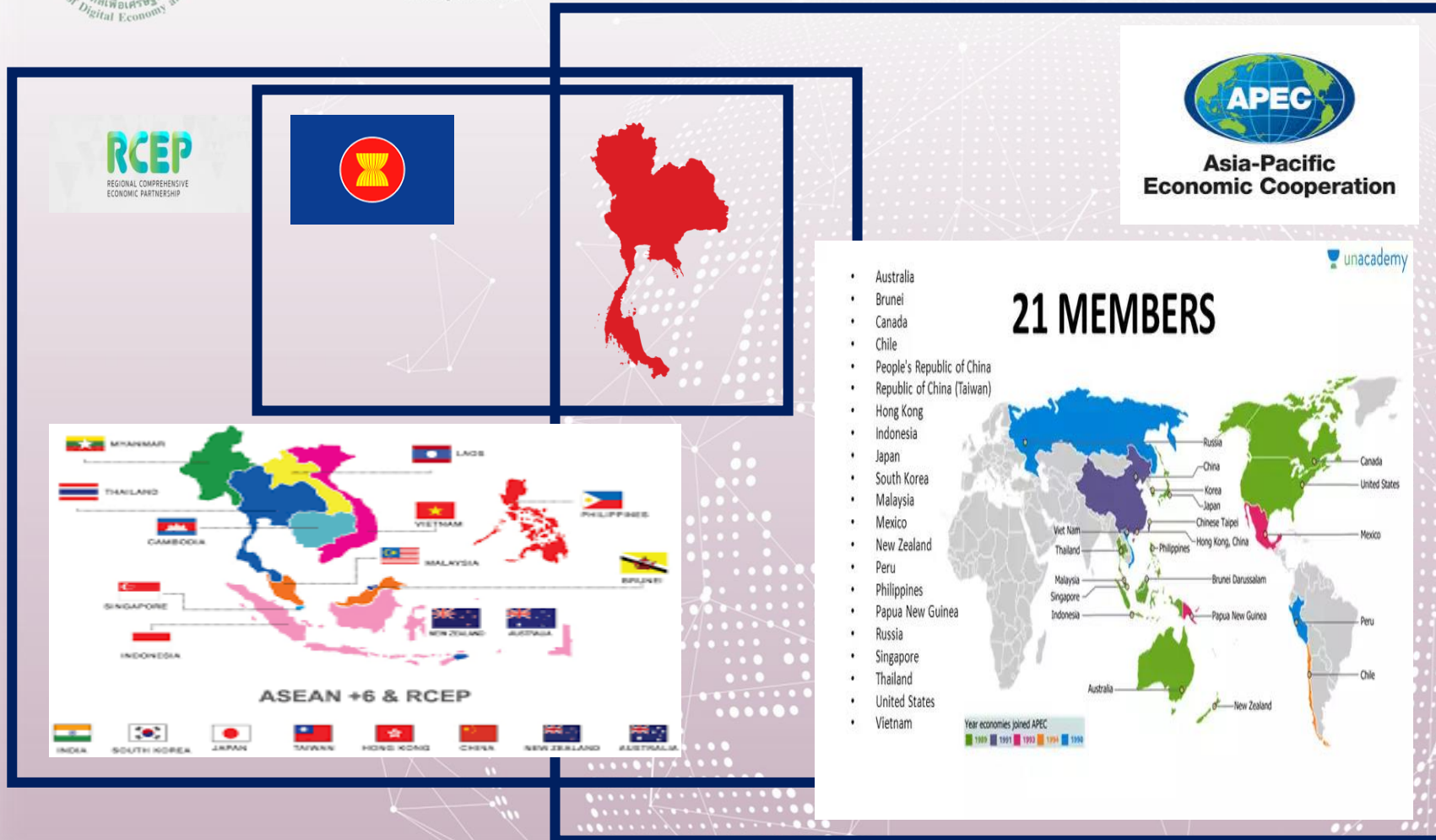
Co-Hosted By



Privacy and data protection eco-system

International and Country Obligation Level

PRIVACY
SECURITY
SUMMIT



✓ **Thailand PDPA (27 May 2019)**

✓ **ASEAN**

Agreement on E-Commerce (Nov18)

✓ **EU GDPR Territorial Scope (May 18)**

✓ **Update E-Privacy Regulation (March 2022)**

✓ **APEC – CBPR /PRP Program**

✓ **RCEP Regional Comprehensive Economic Program (EIF Jan 2022)**

Co-Hosted By



ASEAN agreement on electronic commerce

E-commerce Chapter (Signed 2018)

PRIVACY
SECURITY
SUMMIT

4. Cross-border Transfer of Information by Electronic Means

(a) Member States recognize the importance of allowing information to flow across borders through electronic means, provided that such information shall be used for business purposes, and subject to their respective **laws and regulations**.

(b) Member States agree to facilitate cross-border ecommerce by working towards eliminating or minimizing barriers to the flow of information across borders, including personal information, subject to **appropriate safeguards** to ensure security and confidentiality of information, and when other legitimate public policy objectives so dictate.

(c) Subparagraphs (a) and (b) shall not apply to financial services and financial service suppliers as defined in the Annex on Financial Services of GATS.



Co-Hosted By



Asean agreement on electronic commerce

E-commerce Chapter (Signed 2018)

PRIVACY
SECURITY
SUMMIT

5. Online Personal Information Protection

(a) Each Member State shall adopt or maintain measures to protect the personal information of the users of e-commerce.

(b) A Member State shall not be obliged to implement subparagraph (a) before the date on which that Member **State enacts laws or regulations to protect the personal information of e-commerce users.**

(c) In the development of personal information protection measures, each Member State shall **take into account international principles, guidelines and criteria of relevant international bodies.**



Co-Hosted By



RCEP leaders agree to sign trade pact in 2020

November 7, 2019



PRIVACY
SECURITY
SUMMIT

Regional Comprehensive Economic Partnership: RCEP E-Commerce Chapter (EIF 1 January 2022)

- ประกอบด้วย 17 ข้อบท
- E-Commerce เป็นข้อบทที่เป็น Cross Cutting Issue กับ ทั้ง Trade in Goods, Trade in Services, Financial Services, Financial Service Supplier และ Intellectual Property
- ข้อบทสำคัญที่เกี่ยวข้องกับ Privacy & Security อาทิเช่น Article 12.6: **Electronic Authentication and Electronic Signature**, Article 12.8: **Online Personal Information Protection**, Article 12.13: **Cyber Security**, Article 12.14: **Location of Computing Facilities**, Article 12.15: **Cross-border Transfer of Information by Electronic Means**

Co-Hosted By



Digital Economy Partnership Agreement

Singapore, Chile and New Zealand (Signed 21 January 2020)

PRIVACY
SECURITY
SUMMIT

- ปัจจุบัน ข้อบท E-Commerce นี้ ได้ขยายไปเป็น DEPA – Digital Economy Partnership Agreement ที่ขยายข้อบทออกไปครอบคลุมเรื่องอื่นๆ อาทิเช่น E-Invoicing, Fin-Tech & E-Payment, Open Government Data, Data Innovation and Regulatory Sandbox, AI, SME Cooperation และ Digital Inclusive



Co-Hosted By



CHAPTER 12 ELECTRONIC COMMERCE

SECTION A GENERAL PROVISIONS



Article 12.6: Electronic Authentication and Electronic Signature

1. Except in circumstances otherwise provided for under its laws and regulations, a Party shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form.
2. Taking into account international norms for electronic authentication, each Party shall:
 - (a) **permit** participants in electronic transactions to determine appropriate electronic authentication technologies and implementation models for their electronic transactions;
 - (b) **not limit the recognition** of electronic authentication technologies and implementation models for electronic transactions; and
 - (c) permit participants in electronic transactions to have the **opportunity to prove** that their electronic transactions comply with its laws and regulations with respect to electronic authentication.
3. Notwithstanding paragraph 2, each Party may require that, for a particular category of electronic transactions, the method of electronic authentication **meets certain performance standards or is certified by an authority accredited** in accordance with its laws and regulations.
4. The Parties shall encourage the use of **interoperable** electronic authentication.

Co-Hosted By



CHAPTER 12 ELECTRONIC COMMERCE

SECTION C

CREATING A CONDUCIVE ENVIRONMENT FOR ELECTRONIC COMMERCE

PRIVACY
SECURITY
SUMMIT

Article 12.7: Online Consumer Protection

1. The Parties recognise the importance of adopting and maintaining transparent and effective consumer protection measures for electronic commerce as well as other measures conducive to the development of consumer confidence.
2. Each Party shall adopt or maintain laws or regulations **to provide protection** for consumers using electronic commerce against fraudulent and misleading practices that cause harm or potential harm to such consumers.
3. The Parties recognise the importance of cooperation between their respective competent authorities in charge of consumer protection on activities related to electronic commerce in order to enhance consumer protection.
4. Each Party shall publish information on the consumer protection it provides to users of electronic commerce, including how:
 - (a) **consumers can pursue remedies**; and
 - (b) **business can comply with any legal requirements**.

Co-Hosted By



CHAPTER 12 ELECTRONIC COMMERCE

SECTION C

CREATING A CONDUCIVE ENVIRONMENT FOR ELECTRONIC COMMERCE



Article 12.8: Online Personal Information Protection

1. Each Party shall adopt or maintain a legal framework which ensures the protection of personal information of the users of electronic commerce.
2. In the development of its legal framework for the protection of personal information, each Party **shall take into account international standards, principles, guidelines, and criteria** of relevant international organisations or bodies.
3. Each Party **shall publish information on the personal information protection** it provides to users of electronic commerce, including how:
 - (a) individuals can pursue remedies; and**
 - (b) business can comply with any legal requirements.**
4. The Parties shall encourage juridical persons to publish, including on the internet, their policies and procedures related to the protection of personal information.
5. The Parties shall cooperate, to the extent possible, for the protection of personal information transferred from a Party.

Co-Hosted By



Asia-Pacific Economic Cooperation (APEC)

DESG – Digital Economy Steering Group

DSP Data Privacy Sub-Group

**PRIVACY
SECURITY**
SUMMIT



- **APEC Privacy Framework – 21 Economies**
- **CBPRs** – Cross Border Privacy Rules System – 9 Economies
- **PRP** - APEC PRIVACY RECOGNITION FOR PROCESSORS SYSTEM



Co-Hosted By



**Asia-Pacific
Economic Cooperation**



- The APEC Cross-Border Privacy Rules (CBPR) system, ได้รับโดยผู้นำของกลุ่มประเทศ APEC มาตั้งแต่ปี 2553-11 ปีมาแล้ว
- เป็นระบบที่ประเทศสมาชิก APEC เข้าร่วมโดยความสมัครใจ (voluntary)
- เป็นระบบที่การคุ้มครองข้อมูลส่วนบุคคล เป็นรูปแบบ **accountability-based system** เช่นเดียวกับแนวทาง ของ EU GDPR ที่พัฒนามาจาก Directive 95 ที่เป็นรูปแบบ **Notification**
- ปัจจุบันมี 9 ประเทศ ที่เข้าร่วมใน CBPR แล้ว คือ สหรัฐฯ, เม็กซิโก, ญี่ปุ่น, แคนาดา, สิงคโปร์, เกาหลี, ออสเตรเลีย, จีน-ไต้หวัน, และฟิลิปปินส์
- ประเทศที่แสดงเจตจำนงในการเข้าร่วมแล้วคือ เปรู (2013), เวียดนาม (2018)

Co-Hosted By



APEC CBPR System

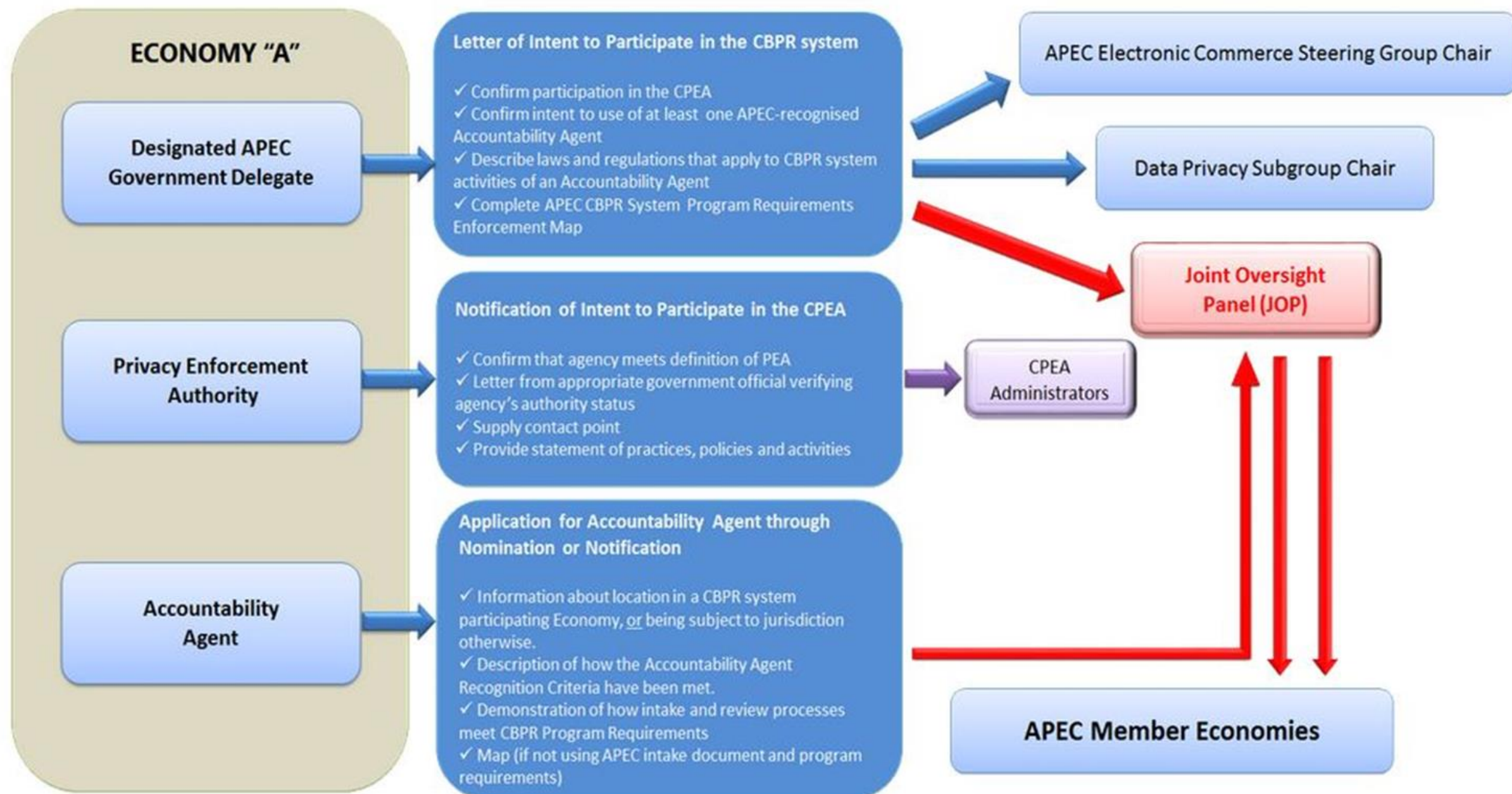
APEC Cross-Border Privacy Rule System (CBPR)

PRIVACY
SECURITY
SUMMIT

The APEC Cross Border Privacy Rules (CBPR) system, endorsed by APEC Leaders in 2011, is a voluntary accountability-based system to facilitate privacy-respecting data flows among APEC economies. It has four main components:

- **recognition criteria** for organizations wishing to become an APEC CBPR system certified Accountability Agent;
- an intake questionnaire for organizations that wish to be certified as APEC CBPR system compliant by a third-party CBPR system certified **Accountability Agent**;
- **assessment criteria** for use by APEC CBPR system certified Accountability Agents when reviewing an organization's answers to the intake questionnaire; and
- a **regulatory cooperative arrangement (the CPEA)** to ensure that each of the APEC CBPR system program requirements can be enforced by participating APEC economies.

Structure of the APEC Cross Border Privacy Rules (CBPR) system



Co-Hosted By



APEC CBPR System

เกี่ยวข้องไปกับ GDPR

PRIVACY
SECURITY
SUMMIT

- EU WP29 ได้ทำงานร่วมกับ APEC – DESG(ECSG) Data Privacy Subgroup มาตั้งแต่ปี 2017 ได้มีการทำงานร่วมกัน ในการหาแนวทางในการใช้มาตรการของ APEC ที่มี เช่น CBPR หรือ PRP มาเป็นกลไกในการ ทำ privacy due diligence ที่เป็นมาตรการให้ EU recognize APEC Privacy Framework
- โอกาสที่ดีของภาคเอกชนไทย เพราะ APEC มีโครงสร้างความร่วมมือในเรื่อง Data Privacy มานาน และมีการดำเนินการในเรื่อง Privacy Framework ที่ได้รับการยอมรับ ที่อ้างอิงใกล้เคียงกับ OECD Privacy Framework.

Co-Hosted By



BCRs and CBPR / PRP

PRIVACY
SECURITY
SUMMIT

- **BCRs – Corporate Binding Rules** เป็นกลไกภายใต้ EU ที่ให้บริษัทข้ามชาติ ที่มีความจำเป็นจะต้องส่งผ่านข้อมูลข้ามแดน ที่กำหนดใน **Article 25** ของ **Directive 95** และ **Article 44** ของ **GDPR** โดยต้อง ทำงานกับ **DPA/DPS** อันใดอันหนึ่งใน EU และ ดำเนินการขึ้นทะเบียน กฎและกระบวนการต่างๆที่ใช้
- **PDPA** ของไทยก็มีการกำหนดในเรื่องที่ใกล้เคียงกับ **BCR** ไว้ในมาตรา 29
- **CBPR** เป็นโครงสร้างที่ **APEC** กำหนดโดยมุ่งหมายให้หน่วยที่เป็น **Controller** แต่ละประเทศในระบบ **CBPR** สามารถรับรอง และยอมรับการรับรองระหว่างกันได้ โดยผ่านกลไกเช่น **Trust Mark** และหน่วยตรวจประเมิน (**Accountability Agent**)
- **PRP – Privacy Recognition for Processor** ที่เป็นกลไกที่มุ่งที่องค์กรต่างๆ ในการที่จะสามารถกำหนด แนวทางในการดำเนินการ ต่อการคุ้มครองข้อมูลส่วนบุคคล ที่มีความสัมพันธ์กับลักษณะธุรกิจ

Co-Hosted By



APEC
PRIVACY RECOGNITION
FOR PROCESSORS SYSTEM
SINGAPORE

PRIVACY
SECURITY
SUMMIT

Organisation Name	Alibaba Cloud (Singapore) Private Limited
Organisation Contact	Takaya Terakawa
Privacy Statement	Visit here
Certification Scope	Processing of data by Alibaba Cloud (Singapore) Private Limited and its subsidiaries (Alibaba Cloud Malaysia, Alibaba Cloud India) through cloud-based services on Alibaba Cloud Platform, for its customers, the controllers.
Initial Certification Date	Apr 2021
Certification Validity Period	Apr 2022 – Apr 2023

Organisation Name	TRS Forensics Pte Ltd
Organisation Contact	Tan Swee Wan
Privacy Statement	Visit here
Certification Scope	Processing of data by TRS Forensics Pte Ltd and its affiliate (TRS Forensics Sdn Bhd) for data forensics related services, for their customers, the controllers
Initial Certification Date	May 2021
Certification Validity Period	May 2022 – May 2023

Organisation Name	Palvision Corporation Pte. Ltd.
Organisation Contact	Patricia Leong
Privacy Statement	Visit here
Certification Scope	Processing of user data by Palvision Corporation Pte. Ltd. and subsidiary (PalVision Inc.) through converged solutions for the hospitality industry
Certification Validity Period	Jan 2022 – Jan 2023

Co-Hosted By



สรุปผลกระทบของพันธกรณีต่างๆ

PRIVACY
SECURITY
SUMMIT

- ก่อให้เกิดมาตรการขั้นต่ำที่ต้องดำเนินการ โดยเฉพาะในกรณีที่เกี่ยวข้องกับเรื่องของ **Privacy** และ **Security** และเปิดโอกาสให้ภาครัฐกิจที่สามารถดำเนินการได้สอดคล้องเปิดโอกาสในการขยายตลาด และมีกิจกรรมบริการบริการ นอกจากนี้จะจำกัดอยู่ภายในประเทศ
- ความชัดเจนในสาระสำคัญ ที่ปรากฏในข้อบท ที่เป็นพันธกรณีที่ต้องดำเนินการว่า ประเด็นใดที่สำคัญที่ต้องดำเนินการ
- มีรูปแบบการส่งเสริมสนับสนุน ที่เป็นรูปธรรม ซึ่งตัวอย่าง **PRP** ของสิงคโปร์นั้น มีการรายงานเมื่อรอบ การประชุมวาระปี 2018 ว่าการที่บริษัทใน สิงคโปร์ที่ได้รับการรับรอง **PRP** ทำให้สามารถไปดำเนินการบริการ หรือกิจกรรมในประเทศในกลุ่ม **APEC** ได้มากขึ้น