



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS//000

Document Classification List

Purpose: Consideration
Submitted by: APEC Secretariat



**Data Privacy Sub-Group Informal Meeting
Ho Chi Minh City, Viet Nam
20 August 2017**

Document Classification List

Document No.	Title	Agenda Item	Submitted By	Public Release		Reason for Restriction	Derestriction Date (where applicable)
				Yes	No		
2017/SOM3/ECSSG/DPS//000	Document Classification List – Data Privacy Sub-Group Informal Meeting 2017	-	APEC Secretariat		√	Internal document	
2017/SOM3/ECSSG/DPS//001	Draft Agenda – Data Privacy Sub-Group Informal Meeting 2017	II	DPS Chair	√			
2017/SOM3/ECSSG/DPS//002	6 th Administration and Accountability Study Group (AASG) Meeting Agenda	II.C	United States	√			
2017/SOM3/ECSSG/DPS//003	Meeting Notes from the 5 th Administration and Accountability Study Group (AASG) Meeting	II.C	United States	√			
2017/SOM3/ECSSG/DPS//004	Communications Strategy for the APEC Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) Systems	II.C	United States	√			
2017/SOM3/ECSSG/DPS//005	Proposed Amendment to Joint Oversight Panel (JOP) Charter	II.C	United States	√			
2017/SOM3/ECSSG/DPS//006	The Guideline of the Common Numbering System to Identify the Cross-Border Privacy Rules (CBPR) Certification Granted by the APEC Recognized Accountability Agent	II.C	United States	√			



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS/II/001

Agenda Item: II

Draft Agenda

Purpose: Consideration
Submitted by: DPS Chair



**Data Privacy Sub-Group Informal Meeting
Ho Chi Minh City, Viet Nam
20 August 2017**

**APEC DATA PRIVACY SUBGROUP
INFORMAL MEETING
AGENDA**

9:00 AM TO 6:00 PM, SUNDAY 20 AUGUST 2017
**Rex Hotel
Ho Chi Minh, Viet Nam**

I. WELCOME AND INTRODUCTION

The Chair will set out the goals for the informal meeting

II. CROSS-BORDER PRIVACY RULES (CBPR) SYSTEM

This item is linked to item 2 of the DPS Meeting agenda

A. Joint Oversight Panel – technical issues for discussion

- a. Joint application for economies and for accountability agents to the CBPR and PRP systems
- b. Other matters

B. CBPR System participants – update on developments and information sharing

- a. Updates from existing economies
- b. Updates from economies working towards participation
- c. Updates from other economies
- d. Discussion of key issues and information sharing opportunities

C. Administration and Accountability Study Group

- a. Website update
- b. Communications plan update
- c. Enforcement update
- d. Other matters

III. UPDATED APEC PRIVACY FRAMEWORK

This item is linked to item 3 of the DPS Meeting agenda

A. Future work options from updates to Privacy Framework

IV. CROSS-BORDER PRIVACY ENFORCEMENT ARRANGEMENT (CPEA)

This item is linked to item 4 of the DPS Meeting agenda

A. Overview of CPEA and benefits - for economies not currently participating

B. Current issues

V. DPS WORK-PLAN

This item is linked to item 7 of the DPS Meeting agenda

A. Future work options from updates to Privacy Framework

B. Opportunities for work options in digital economy matters

VI. CONCLUSION AND NEXT STEPS



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS/II/002

Agenda Item: II.C

Administration and Accountability Study Group Meeting Agenda

Purpose: Information
Submitted by: United States



**Data Privacy Sub-Group Informal Meeting
Ho Chi Minh City, Viet Nam
20 August 2017**

AASG Meeting #6 Agenda

August 20, 2017

- I. Communications work stream**
 - A. Update on website enhancement project**
 - B. Proposed Amendment to JOP Charter on Website Responsibilities**
 - C. Communications Plan**

- II. Accountability work stream**
 - A. Unified numbering system proposal**

- III. Next Steps**



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS/II/003

Agenda Item: II - C

**Meeting Notes from the 5th Administration and
Accountability Study Group Meeting**

Purpose: Information
Submitted by: United States



**Data Privacy Sub-Group Informal Meeting
Ho Chi Minh City, Viet Nam
20 August 2017**

Meeting Notes from AASG Meeting #5

April 27/28, 2017

Participants

- Participating Economies:
 - Australia: Attorney-General's Department (AG)
 - Canada: Office of the Privacy Commissioner (OPC)
 - Chinese Taipei: Bureau of Foreign Trade (BOFT); Department of Commerce, Ministry of Economic Affairs (MOEA); Ministry of Justice (MOJ); Institute for Information Industry (III)
 - Japan: Ministry of Economy, Trade, and Industry (METI); Personal Information Protection Commission (PPC)
 - Singapore: Personal Data Protection Commission (PDPC)
 - United States: Department of Commerce (DoC); Federal Trade Commission (FTC)
- Participating Accountability Agents: TRUSTe, JIPDEC
- Participating Private Sector: Centre for Information Policy Leadership (CIPL), Cisco

Discussion Summary

Website Administration:

- DoC proposed amending the "Administrative Matters" section of the JOP Charter to clarify responsibilities for the cbprs.org website. Feedback on the proposed amendment included:
 - ensuring that the language applies to both the CBPR and PRP aspects of the site (FTC),
 - considering different placement (either within the Charter or in a different document) for the website administration language (OPC will follow up with a suggestion in writing),
 - Clarifying whether the host and domain holder can be replaced at the JOP Chair's discretion (AG), and
 - Developing and submitting a proposal to the ECSG Chair for consideration at SOM 3 in Ho Chi Minh City (METI).

Communications Plan:

- DoC presented its draft text for a CBPR and PRP Communications Plan for the AASG's consideration. Ideas for the draft plan included:
 - seeking the APEC Secretariat's assistance developing publications on behalf of the ECSG (AG),
 - surveying DPS and ECSG members about difficulties they encounter in understanding and explaining the CBPR and PRP systems in order to develop FAQs to be posted on the CBPR website in advance of SOM 3 (OPC),
 - including a mechanism on the CBPR website for people to ask general questions (CIPL), and
 - ensuring that Economies can add specific content to the website (FTC).

Common Numbering System:

- Japan will circulate a proposal to AASG members for comment in advance of the next meeting.

Enforcement Jurisdiction Project:

- The FTC is analyzing its own jurisdictional reach in regards to enforcement of the CBPR and PRP systems and hopes to report its findings on the next AASG call.

General Announcements:

- Chinese Taipei will hold a CBPR seminar with a focus on awareness-raising on October 2, 2017, and will circulate a draft agenda soon and solicit the AASG's feedback.
- Japan noted that CIPL will be hosting a workshop about the CBPR system in Tokyo in May 2017, and that Japan is also working with Vietnam to host a CBPR-related workshop on the margins of SOM 3 in Ho Chi Minh City in August 2017.
- Japan reported that its amended Act on the Protection of Personal Information (APPI) will enter into force on May 30, and the PPC will become Japan's consolidated PEA. On April 27, PPC submitted its application to join the CPEA.

Next Steps:

- DoC will propose a date for a meeting in June and will circulate a draft agenda to participants.



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS/II/004

Agenda Item: II.C

Communications Strategy for the APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems

Purpose: Information
Submitted by: United States



**Data Privacy Sub-Group Informal Meeting
Ho Chi Minh City, Viet Nam
20 August 2017**

DRAFT—NOT FOR PUBLIC DISTRIBUTION

COMMUNICATIONS STRATEGY FOR THE APEC CROSS-BORDER PRIVACY RULES (CBPR) AND PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEMS

Background & Purpose

While the APEC Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems are expanding, the systems and their benefits are not well understood by businesses and consumers. The purpose of this plan is to lay out key messages about the CBPR and PRP systems and ensure that those messages are communicated with clarity and consistency.

Audience

The audience for these communications is those participating in, considering participating in, or seeking to learn about the CBPR and PRP systems, including governments, enforcement authorities, consumers, companies and Accountability Agents.

Communications Goals

- 1) To explain clearly and concisely what the CBPR and PRP systems are, their importance, and how they work, and
- 2) to highlight the benefits of the CBPR and PRP systems to various stakeholders

Communications Tactics

- 1) **Enhance the cbprs.org website** by providing clear, easy to navigate information to consumers and businesses about the CBPR and PRP systems and how they address complaints. Provide a mechanism on the website for people to ask general questions, and ensure that members can add economy-specific content to the site,
- 2) **Develop print publications and a distribution plan for them** (with the assistance of the Secretariat, if possible), including one-pagers that concisely communicate the purpose and benefits of the CBPR and PRP systems and direct readers to the website for more information,
- 3) **Publish a public version of the updated APEC Privacy Framework**, which provides the foundation of the systems,
- 4) **Host workshops and webinars** geared toward educating economies, enforcement authorities and companies about the CBPR and PRP systems and how to implement them,
- 5) **Conduct outreach at other events** that are to be held in interested and participating CBPR economies, at which the AASG could potentially participate and highlight CBPR, and
- 6) **Develop Frequently Asked Questions (FAQs)** to be posted on the website, based on discussions with stakeholders about the difficulties they encounter in understanding and explaining the CBPR and PRP systems.

Messaging

The AASG will develop clear and consistent messages regarding:

- The purpose of the CBPR and PRP systems,
- how the systems work,
- the benefits of the CBPR system for businesses, and information on the certification process, including “typical” time for CBPR certification, costs associated with certification, and testimonials of the benefits delivered to certified companies,
- the benefits of the CBPR system for consumers,
- the benefits of the CBPR system for governments and regulators,
- how businesses can participate in the CBPR system, and
- what consumers can expect from certified organizations and how they can address complaints



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS/II/005

Agenda Item: II.C

Proposed Amendment to Joint Oversight Panel Charter

Purpose: Information
Submitted by: United States



**Data Privacy Sub-Group Informal Meeting
Ho Chi Minh City, Viet Nam
20 August 2017**

DRAFT--Proposed Amendment to JOP Charter

7. ADMINISTRATIVE MATTERS

7.1 The Chairperson of the Joint Oversight Panel will provide a summary report detailing all activities carried out by the Joint Oversight Panel under paragraph 6 to the Data Privacy Subgroup Chair no later than one month in advance of each Data Privacy Subgroup meeting.

7.2 The initial terms of membership for the initial Joint Oversight Panel are as follows:

- i. One Chair to be appointed for a two-year term;
- ii. One member to be appointed for an 18 month-term, and;
- iii. One member to be appointed for a one-year term.

7.3 Upon expiration of the initial term, each appointment will have a two-year term subject to re-appointment at the discretion of the ECSG based on 6.1.

7.4 The content on the CBPR website is to be updated and maintained by the JOP Chair or by the JOP Chair's designee. The JOP Chair shall also designate (1) a host for the website and (2) a domain holder who shall be responsible for buying, holding and renewing the domain name.



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS/II/006

Agenda Item: II.C

**The Guideline of the Common Numbering System to
Identify the Cross-Border Privacy Rules Certification
Granted by the APEC Recognized Accountability
Agent**

Purpose: Information
Submitted by: United States



**Data Privacy Sub-Group Informal Meeting
Ho Chi Minh City, Viet Nam
20 August 2017**

**The Guideline of the Common Numbering System to Identify the CBPR Certification Granted by the APEC
Recognized Accountability Agent**
(Draft)

This guideline specifies the example of the APEC CBPR certification number and rules of the common numbering system to identify the CBPR certification issued by the APEC Recognized Accountability Agent.

Example of the APEC CBPR Certification Number;

“XX01-00001-01”

1. The common number consists of three parts that are connected by a dash.
2. The first part composed of a set of two letters and a set of two digits. The first set of two letters is the abbreviation of the name of the economy where Accountability Agent is located and the second set of two digits is the serial number of the recognized Accountability Agents in that economy. The rule how to abbreviate economies name should conform to the “ISO 3166-1, *Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes*” or equivalent national standards. For example, “JP” stands for Japan and “US” stands for the United States and in Japan “01” is the designated number of the JIPDEC and also explains the JIPDEC is the first recognized Accountability Agent in Japan.
3. The second part consists of a set of five digits and is the serial number of the certified organization designated by the Accountability Agent. For example, “00001” shows this organization is the first organization of which the CBPR certification is granted.
4. The last part consists of a set of two digits and is the number of the CBPR certification granted to this organization. For example, “01” shows that this is the first certification of that organization.
5. Once the Accountability Agent is recognized by the ECSG, the proposing economy should designate two digits serial number of the recognized Accountability Agent and report the number and name of the Accountability Agent to the chair of the Joint Oversight Panel. The Joint Oversight Panel maintains and makes public the list of the number of the Accountability Agent designated by the proposing economy with the name of the economy based on the reported information from the proposing economy.
6. This guideline should apply both a paper format and an electronic format of the certifications and this number may be appeared on the paper certificate or the website.

Note: Five digits serial number of certified organization stipulated point 3 and two digits serial number of recognized Accountability Agents stipulated in point 5 are expandable when the number of certified companies or recognized Accountability Agents will exceed 99999 or 99 respectively in each economy.



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS/000

Document Classification List

Purpose: Consideration
Submitted by: APEC Secretariat



**Data Privacy Sub-Group Meeting
Ho Chi Minh City, Viet Nam
21 August 2017**

Document Classification List

Document No.	Title	Agenda Item	Submitted By	Public Release		Reason for Restriction	Derestriction Date (where applicable)
				Yes	No		
2017/SOM3/ECSSG/DPS/000	Document Classification List – Data Privacy Sub-Group Meeting 2017	-	APEC Secretariat		√	Internal document	
2017/SOM3/ECSSG/DPS/001	Draft Agenda – Data Privacy Sub-Group Meeting 2017	1(a)	DPS Chair	√			
2017/SOM3/ECSSG/DPS/002	Terms of Reference for Cross-Border Privacy Rules Enhancements	2(b), 5(b)	United States	√			
2017/SOM3/ECSSG/DPS/003	Personal Information Protection Commission	2(b)	Japan	√			
2017/SOM3/ECSSG/DPS/004	Workshop for Promotion of the APEC Cross-Border Privacy Rules (CBPR) System	2(b)	Japan	√			
2017/SOM3/ECSSG/DPS/005	6 th Administration and Accountability Study Group (AASG) Meeting Agenda	2(e)	United States	√			
2017/SOM3/ECSSG/DPS/006	Meeting Notes from 5 th Administration and Accountability Study Group (AASG)	2(e)	United States	√			
2017/SOM3/ECSSG/DPS/007	Communications Strategy for the APEC Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) Systems	2(e)	United States	√			
2017/SOM3/ECSSG/DPS/008	Proposed Amendment to Joint Oversight Panel (JOP) Charter	2(e)	United States	√			
2017/SOM3/ECSSG/DPS/009	The Guideline of the Common Numbering System to Identify the Cross-Border Privacy Rules (CBPR) Certification Granted by the APEC Recognized Accountability Agent	2(e)	United States	√			
2017/SOM3/ECSSG/DPS/010	Discussion Paper: Certifications, Seals and Marks Under the General Data Protection Regulation (GDPR) and Their Roles As Accountability Tools and Cross-Border Data Transfer Mechanisms	9(a)	CIPL	√			
2017/SOM3/ECSSG/DPS/011	Report Data Privacy Sub-Group Meeting, 23 February 2017, Nha Trang, Viet Nam	1(b)	APEC Secretariat		√		
2017/SOM3/ECSSG/DPS/012	Global Industry Calls for Rapid and Ambitious Expansion of Participation in the APEC Cross-Border Privacy Rules System	9(a)	ITI	√			



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS/001

Agenda Item: 1(a)

Draft Agenda

Purpose: Consideration
Submitted by: DPS Chair



**Data Privacy Sub-Group Meeting
Ho Chi Minh City, Viet Nam
21 August 2017**

**36TH APEC ELECTRONIC COMMERCE STEERING GROUP MEETING
DATA PRIVACY SUB-GROUP MEETING
AGENDA**

9:00 AM TO 6:00 PM, MONDAY 21 AUGUST 2017

**Rex Hotel
Ho Chi Minh, Viet Nam**

1) INTRODUCTION AND ADMINISTRATION

- (a) The Chair will request **approval** of the agenda
- (b) **Noting and approval** of 35th DPS meeting report
- (c) DPS Executive positions – **for decision** - vice-chair position

2) CROSS BORDER PRIVACY RULES (CBPR) SYSTEM

- (a) Report from Joint Oversight Panel Chair – **United States**
 - i. Current matters under JOP consideration
 - ii. Joint application process for CBPR and PRP systems
 - A. For economies
 - B. For accountability agents
 - iii. Opportunity for Economies to communicate Intent to Participate
- (b) Updates from existing CBPR economy participants – **United States, Japan, Mexico, Canada, Korea**
- (c) Updates from economies working towards participation – **Singapore, Chinese Taipei, Philippines**
- (d) Updates from economies considering participation - **Australia**
- ✓ (e) Administration and Accountability Study Group – **United States**
 - i. Common numbering system for CBPR certification - **Japan**
 - ii. Website update
 - iii. Communications plan update
 - iv. Enforcement update
 - v. Other matters

3) UPDATED APEC PRIVACY FRAMEWORK

- (a) For **discussion**: possible areas of future work for DPS
- (b) Study Group in data portability

4) CROSS BORDER PRIVACY ENFORCEMENT ARRANGEMENT (CPEA)

- (a) Overview of CPEA and participation by member economies – **United States**
- (b) Update on recent developments by administrators – **United States**

5) APEC PROJECTS

- (a) Project Management Update - the **APEC Secretariat**
- (b) Update on Multi-Year Project - CBPR System Capacity Building and Administrative Support
 - i. Status Report from MYP Project Lead – **United States**
- (c) Report on Public Private Dialogue on Facilitating MSME adoption of cross-border e-commerce – **Viet Nam**

- (d) Capacity-Building for Compliance with Cross-Border Privacy Rules System in APEC - Chinese Taipei

6) UPDATED DATA PRIVACY INDIVIDUAL ACTION PLANS

- (a) Chair will invite economies to submit a new IAP or update their existing IAP using the revised IAP template

7) DPS 2017 WORK PLAN

- (a) The Chair will lead a discussion reviewing the 2017 Work Plan for preparation of 2018 version
- (b) **Discussion and decision** on Work Plan

8) REPORTS FROM SUB-GROUP MEMBER ECONOMIES

- (a) Member Economies of the Sub-Group are invited to provide a brief (3 minute) report on relevant data privacy developments.

i. Russia

9) INFORMATION SHARING ON CROSS-BORDER PRIVACY ISSUES

- (a) Guests are invited to provide a brief (3 minute) report on relevant data privacy developments

ii. the Information Technology Industry Council (ITI)

- (b) Report on developments in:

- i. the International Conference of Data Protection and Privacy Commissioners (ICDPPC) HK
- ii. the Asia Pacific Privacy Authorities Forum (APPA) US
- iii. the Global Privacy Enforcement Network (GPEN)
- iv. the APEC E-Commerce Business Alliance (ECBA)

10) CONCLUSION AND NEXT STEPS FOR THE DATA PRIVACY SUB-GROUP

- (a) Members will have the opportunity to inform the Sub-Group of any other matters by prior arrangement with the Chair
- (b) **Review and decision** - Meeting document access
- (c) The Chair will provide a verbal summary of the meeting that will form the basis for the Chair's report to the ECSG



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS/002

Agenda Item: 2(b), 5(b)

Terms of Reference for Cross-Border Privacy Rules Enhancements

Purpose: Information
Submitted by: United States



**Data Privacy Sub-Group Meeting
Ho Chi Minh City, Viet Nam
21 August 2017**

TERMS OF REFERENCE FOR CBPRS.ORG ENHANCEMENTS

1. Background

APEC developed the APEC Cross-Border Privacy Rules (CBPR) and the APEC Privacy Recognition for Processors (PRP) to enhance consumer, business, and regulator trust and accountability with respect to the cross border flow of personal information. APEC economies are now in the process of implementing the CBPR and PRP systems across the APEC region and are working to promote the systems' business and consumer benefits.

2. Objective

This project is intended to improve the cbprs.org website in order to entice economies and businesses to participate in the CBPR and PRP systems, provide information and support for those already participating in the systems, and provide transparency to entities, including consumers, about how the systems operate. The audience for the enhanced website includes those currently participating in, considering participating in, or seeking to learn about, the CBPR system, including governments, enforcement authorities, consumers, companies, and Accountability Agents. The enhancements will be designed to make the website more informative, attractive, and easy to use for its audience.

3. Scope/Task of Contractors

The contractor is expected to work in consultation with the Project Overseer to improve the cbprs.org website, including the following specific enhancements:

- (1) update the website's overall appearance;
- (2) post all endorsed CBPR and PRP system documents and related documents, including economy and accountability agent applications.
- (3) provide clear, easy-to-navigate information, including written descriptions, forms, templates, graphics and figures, to consumers and businesses about the CBPR System, including how it works, how it can be used and how it addresses complaints, including those involving false claims about CBPR or PRP certification in each participating economy and in APEC as a whole;
- (4) create a searchable, consumer-friendly directory of certified companies that Accountability Agents can update directly with relevant information, such as logos and links to company privacy policies;
- (5) create a complaint assistant on the website where consumers can enter complaints, which would be directed to the appropriate party;
- (6) post a list of the Cross Border Privacy Enforcement Authorities with appropriate contact information;
- (7) incorporate a news feed for posting developments in the CBPR and PRP Systems and an events calendar for posting upcoming CBPR and PRP-related events.

The contractor is expected to implement appropriate security measures, including secure protocols.

Before commencing work on the site, the contractor is expected to provide the Project Overseer and the APEC Secretariat with (1) a work plan specifying the work to be completed on the site and the estimated cost and timeframe for completing each item and (2) mock-ups demonstrating the look and content of the site's redesign. The contractor is also expected to report to the Project Overseer and APEC Secretariat each week describing (1) work completed, (2) any necessary modifications to the work plan, and (3) work expected to be completed over the subsequent week. At the conclusion of the project, the contractor is expected to submit a report outlining (1) all work completed, (2) modifications to the initial work plan, (3) lessons learned, (4) and a cost estimate for ongoing maintenance and operations.

The contractor is expected to conduct a demonstration of the new site at APEC Senior Officials Meeting 3, to be held in Ho Chi Minh City, Vietnam in August 2017.

4. Duration and Phasing

Prepare work plan and mock-ups
Format: Document

Delivery Date: April 28, 2017

Finalize enhanced website
Format: Website
Delivery Date: July 28, 2017

Demonstration of website
Format: Workshop/Presentation
Delivery Date: August, 2017

Prepare a written report outlining work completed
Format: Document
Delivery Date: September 18, 2017

5. Specifications of Skill Sets and Experience

Contractors should have experience designing professional websites for large organizations.

6. Reporting Requirements

1) Delivery of work plan and initial design mock-ups
Due Date: April 28, 2017
Means of Verification: Receipt of documents

2) Delivery of weekly progress reports
Due Dates: Weekly, from May 5 through July 21 or completion of project
Means of Verification: Receipt of progress report

4) Finalize enhanced website
Due Date: July 28, 2017
Means of Verification: Completed website

5) Delivery of final report
Due Date: September 18, 2017
Means of Verification: Receipt of report

All documents produced should conform to APEC publication guidelines.



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS/003

Agenda Item: 2(b)

Personal Information Protection Commission

Purpose: Information
Submitted by: Japan



**Data Privacy Sub-Group Meeting
Ho Chi Minh City, Viet Nam
21 August 2017**

What is the PPC?

History

- Jan 2014 The Specific Personal Information Protection Commission (SPPC) was established
- Jan 2016 The Personal Information Protection Commission was established (into which the SPPC was merged)

Function under the Jurisdiction

- (1) Affairs related to specific personal information
(monitoring/supervision, specific personal information protection assessment)
- (2) Affairs related to the APPI (Holding jurisdiction over the APPI)
(Affairs related to monitoring/supervision based on the Amended APPI is to be added after its full enforcement.)
- (3) Affairs common to (1) and (2)
(public relations/an enlightenment campaign, international cooperation etc.)

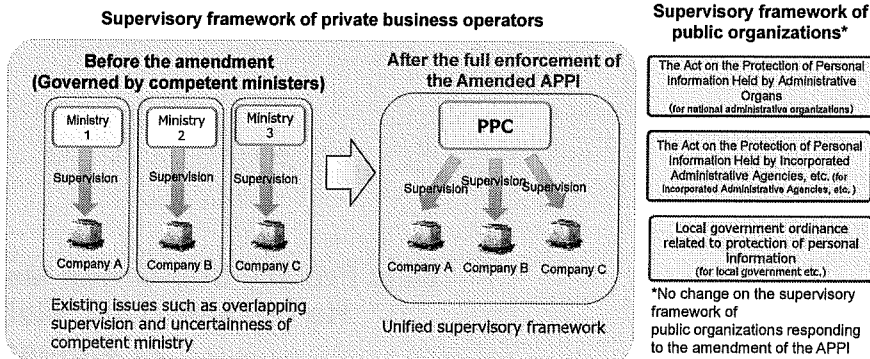
Organizational Structure

- A collegial decision-making body comprising one chairperson and eight commissioners (Administrative commission)
- The chairperson and eight commissioners exercise their official authorities independently (with terms of five years)
- The number of professional staff of the PPC secretariat : 127 (as of 1 August, 2017)



Establishment of the PPC

- Centralization of regulatory authorities currently hold by respective business jurisdictional ministers to the PPC at the time of full enforcement of the Amended APPI
- Authorized to require a business operator to report or conduct on-site inspection as necessary, and in addition, to provide with guidance or advice, or to recommend or order in accordance with actual circumstances



The APEC CBPR system

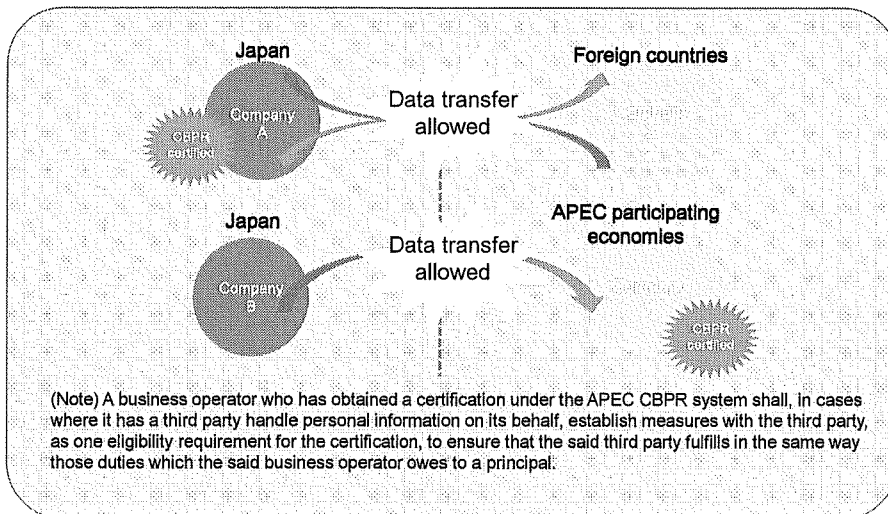
➤ CBPR system promotion activities by Personal Information Protection Commission, Japan

- ✓ Participated in the Administration and Accountability Study Group established under the APEC Data Privacy Subgroup (DPS)
- ✓ Produced CBPR promotion brochures and put them on the PPC webpage
- ✓ Held explanatory seminars on the CBPR
on a total of 90 occasions attended by about 13,020 people
- ✓ Provided a presentation at various conferences
International Conference of Data Protection and Privacy Commissioners (ICDPPC),
Asia Pacific Privacy Authorities (APPA) Forum, etc.

8

The APEC CBPR system

➤ CBPR system and the Act on the Protection of Personal Information (APPI)



6



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS/004

Agenda Item: 2(b)

Workshop for Promotion of the APEC Cross-Border Privacy Rules System

Purpose: Information

Submitted by: Japan



**Data Privacy Sub-Group Meeting
Ho Chi Minh City, Viet Nam
21 August 2017**



WORKSHOP FOR PROMOTION OF THE APEC/CBPR SYSTEM

*Host: Personal Information Protection Commission
(PPC), Japan*

Time: 13:30-15:00, 27 September, 2017

*Venue: Magnolia (Lower Level II),
Kowloon Shangri-La Hotel*

Tentative Agenda

- **Outline, Purpose and Prospect of the CBPR system**
- **Lectures targeted for government stakeholders**
- **Lectures targeted for business operators**
- **Panel Discussion**



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS/005

Agenda Item: 2(e)

6th Administration and Accountability Study Group Meeting Agenda

Purpose: Information
Submitted by: United States



**Data Privacy Sub-Group Meeting
Ho Chi Minh City, Viet Nam
21 August 2017**

AASG Meeting #6 Agenda

August 20, 2017

- I. Communications work stream**
 - A. Update on website enhancement project**
 - B. Proposed Amendment to JOP Charter on Website Responsibilities**
 - C. Communications Plan**

- II. Accountability work stream**
 - A. Unified numbering system proposal**

- III. Next Steps**



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS/006

Agenda Item: 2(e)

Meeting Notes from 5th Administration and Accountability Study Group

Purpose: Information
Submitted by: United States



**Data Privacy Sub-Group Meeting
Ho Chi Minh City, Viet Nam
21 August 2017**

Meeting Notes from AASG Meeting #5

April 27/28, 2017

Participants

- Participating Economies:
 - Australia: Attorney-General's Department (AG)
 - Canada: Office of the Privacy Commissioner (OPC)
 - Chinese Taipei: Bureau of Foreign Trade (BOFT); Department of Commerce, Ministry of Economic Affairs (MOEA); Ministry of Justice (MOJ); Institute for Information Industry (III)
 - Japan: Ministry of Economy, Trade, and Industry (METI); Personal Information Protection Commission (PPC)
 - Singapore: Personal Data Protection Commission (PDPC)
 - United States: Department of Commerce (DoC); Federal Trade Commission (FTC)
- Participating Accountability Agents: TRUSTe, JIPDEC
- Participating Private Sector: Centre for Information Policy Leadership (CIPL), Cisco

Discussion Summary

Website Administration:

- DoC proposed amending the "Administrative Matters" section of the JOP Charter to clarify responsibilities for the cbprs.org website. Feedback on the proposed amendment included:
 - ensuring that the language applies to both the CBPR and PRP aspects of the site (FTC),
 - considering different placement (either within the Charter or in a different document) for the website administration language (OPC will follow up with a suggestion in writing),
 - Clarifying whether the host and domain holder can be replaced at the JOP Chair's discretion (AG), and
 - Developing and submitting a proposal to the ECSG Chair for consideration at SOM 3 in Ho Chi Minh City (METI).

Communications Plan:

- DoC presented its draft text for a CBPR and PRP Communications Plan for the AASG's consideration. Ideas for the draft plan included:
 - seeking the APEC Secretariat's assistance developing publications on behalf of the ECSG (AG),
 - surveying DPS and ECSG members about difficulties they encounter in understanding and explaining the CBPR and PRP systems in order to develop FAQs to be posted on the CBPR website in advance of SOM 3 (OPC),
 - including a mechanism on the CBPR website for people to ask general questions (CIPL), and
 - ensuring that Economies can add specific content to the website (FTC).

Common Numbering System:

- Japan will circulate a proposal to AASG members for comment in advance of the next meeting.

Enforcement Jurisdiction Project:

- The FTC is analyzing its own jurisdictional reach in regards to enforcement of the CBPR and PRP systems and hopes to report its findings on the next AASG call.

General Announcements:

- Chinese Taipei will hold a CBPR seminar with a focus on awareness-raising on October 2, 2017, and will circulate a draft agenda soon and solicit the AASG's feedback.
- Japan noted that CIPL will be hosting a workshop about the CBPR system in Tokyo in May 2017, and that Japan is also working with Vietnam to host a CBPR-related workshop on the margins of SOM 3 in Ho Chi Minh City in August 2017.
- Japan reported that its amended Act on the Protection of Personal Information (APPI) will enter into force on May 30, and the PPC will become Japan's consolidated PEA. On April 27, PPC submitted its application to join the CPEA.

Next Steps:

- DoC will propose a date for a meeting in June and will circulate a draft agenda to participants.



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS/007

Agenda Item: 2(e)

**Communications Strategy for the APEC Cross-
Border Privacy Rules and Privacy Recognition for
Processors Systems**

Purpose: Information
Submitted by: United States



**Data Privacy Sub-Group Meeting
Ho Chi Minh City, Viet Nam
21 August 2017**

DRAFT—NOT FOR PUBLIC DISTRIBUTION

COMMUNICATIONS STRATEGY FOR THE APEC CROSS-BORDER PRIVACY RULES (CBPR) AND PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEMS

Background & Purpose

While the APEC Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems are expanding, the systems and their benefits are not well understood by businesses and consumers. The purpose of this plan is to lay out key messages about the CBPR and PRP systems and ensure that those messages are communicated with clarity and consistency.

Audience

The audience for these communications is those participating in, considering participating in, or seeking to learn about the CBPR and PRP systems, including governments, enforcement authorities, consumers, companies and Accountability Agents.

Communications Goals

- 1) To explain clearly and concisely what the CBPR and PRP systems are, their importance, and how they work, and
- 2) to highlight the benefits of the CBPR and PRP systems to various stakeholders

Communications Tactics

- 1) **Enhance the cbprs.org website** by providing clear, easy to navigate information to consumers and businesses about the CBPR and PRP systems and how they address complaints. Provide a mechanism on the website for people to ask general questions, and ensure that members can add economy-specific content to the site,
- 2) **Develop print publications and a distribution plan for them** (with the assistance of the Secretariat, if possible), including one-pagers that concisely communicate the purpose and benefits of the CBPR and PRP systems and direct readers to the website for more information,
- 3) **Publish a public version of the updated APEC Privacy Framework**, which provides the foundation of the systems,
- 4) **Host workshops and webinars** geared toward educating economies, enforcement authorities and companies about the CBPR and PRP systems and how to implement them,
- 5) **Conduct outreach at other events** that are to be held in interested and participating CBPR economies, at which the AASG could potentially participate and highlight CBPR, and
- 6) **Develop Frequently Asked Questions (FAQs)** to be posted on the website, based on discussions with stakeholders about the difficulties they encounter in understanding and explaining the CBPR and PRP systems.

Messaging

The AASG will develop clear and consistent messages regarding:

- The purpose of the CBPR and PRP systems,
- how the systems work,
- the benefits of the CBPR system for businesses, and information on the certification process, including "typical" time for CBPR certification, costs associated with certification, and testimonials of the benefits delivered to certified companies,
- the benefits of the CBPR system for consumers,
- the benefits of the CBPR system for governments and regulators,
- how businesses can participate in the CBPR system, and
- what consumers can expect from certified organizations and how they can address complaints



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS/008

Agenda Item: 2(e)

Proposed Amendment to Joint Oversight Panel Charter

Purpose: Information
Submitted by: United States



**Data Privacy Sub-Group Meeting
Ho Chi Minh City, Viet Nam
21 August 2017**

DRAFT--Proposed Amendment to JOP Charter

7. ADMINISTRATIVE MATTERS

7.1 The Chairperson of the Joint Oversight Panel will provide a summary report detailing all activities carried out by the Joint Oversight Panel under paragraph 6 to the Data Privacy Subgroup Chair no later than one month in advance of each Data Privacy Subgroup meeting.

7.2 The initial terms of membership for the initial Joint Oversight Panel are as follows:

- i. One Chair to be appointed for a two-year term;
- ii. One member to be appointed for an 18 month-term, and;
- iii. One member to be appointed for a one-year term.

7.3 Upon expiration of the initial term, each appointment will have a two-year term subject to re-appointment at the discretion of the ECSG based on 6.1.

7.4 The content on the CBPR website is to be updated and maintained by the JOP Chair or by the JOP Chair's designee. The JOP Chair shall also designate (1) a host for the website and (2) a domain holder who shall be responsible for buying, holding and renewing the domain name.



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS/009

Agenda Item: 2(e)

**The Guideline of the Common Numbering System to
Identify the Cross-Border Privacy Rules Certification
Granted by the APEC Recognized Accountability
Agent**

Purpose: Information
Submitted by: United States



**Data Privacy Sub-Group Meeting
Ho Chi Minh City, Viet Nam
21 August 2017**

**The Guideline of the Common Numbering System to Identify the CBPR Certification Granted by the APEC
Recognized Accountability Agent**

(Draft)

This guideline specifies the example of the APEC CBPR certification number and rules of the common numbering system to identify the CBPR certification issued by the APEC Recognized Accountability Agent.

Example of the APEC CBPR Certification Number;

“XX01-00001-01”

1. The common number consists of three parts that are connected by a dash.
2. The first part composed of a set of two letters and a set of two digits. The first set of two letters is the abbreviation of the name of the economy where Accountability Agent is located and the second set of two digits is the serial number of the recognized Accountability Agents in that economy. The rule how to abbreviate economies name should conform to the “ISO 3166-1, *Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes*” or equivalent national standards. For example, “JP” stands for Japan and “US” stands for the United States and in Japan “01” is the designated number of the JIPDEC and also explains the JIPDEC is the first recognized Accountability Agent in Japan.
3. The second part consists of a set of five digits and is the serial number of the certified organization designated by the Accountability Agent. For example, “00001” shows this organization is the first organization of which the CBPR certification is granted.
4. The last part consists of a set of two digits and is the number of the CBPR certification granted to this organization. For example, “01” shows that this is the first certification of that organization.
5. Once the Accountability Agent is recognized by the ECSG, the proposing economy should designate two digits serial number of the recognized Accountability Agent and report the number and name of the Accountability Agent to the chair of the Joint Oversight Panel. The Joint Oversight Panel maintains and makes public the list of the number of the Accountability Agent designated by the proposing economy with the name of the economy based on the reported information from the proposing economy.
6. This guideline should apply both a paper format and an electronic format of the certifications and this number may be appeared on the paper certificate or the website.

Note: Five digits serial number of certified organization stipulated point 3 and two digits serial number of recognized Accountability Agents stipulated in point 5 are expandable when the number of certified companies or recognized Accountability Agents will exceed 99999 or 99 respectively in each economy.



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSSG/DPS/010

Agenda Item: 9(a)

**Discussion Paper: Certifications, Seals and Marks
Under the General Data Protection Regulation and
Their Roles As Accountability Tools and Cross-
Border Data Transfer Mechanisms**

Purpose: Information

Submitted by: Centre of Information Policy Leadership



**Data Privacy Sub-Group Meeting
Ho Chi Minh City, Viet Nam
21 August 2017**

EXECUTIVE SUMMARY

Certifications, seals and marks have the potential to play a significant role in enabling companies to achieve and demonstrate organisational accountability and, more specifically, GDPR compliance for some or all of their services, products or activities. The capability of certifications to provide a comprehensive GDPR compliance structure will be particularly useful for SMEs. For large and multinational companies, certifications may, in addition, facilitate business arrangements with business partners and service providers.

In addition, certifications, seals and marks can be used as accountable, safe and efficient cross-border data transfer mechanisms under the GDPR, provided they are coupled with binding and enforceable commitments, including with regard to data subject rights. Finally, there is potential for creating interoperability with other legal regimes, as well as with similar certifications, seals and marks in other regions or in other policy domains.

These instruments present real benefits for all stakeholders, including DPAs and, most importantly, individuals. They have the potential to assist organisations in delivering better compliance and more effective protection for individuals given that certified organisations will have made a conscious effort to become GDPR compliant and will have been reviewed by a third party in that respect.

However, it is crucial that certifications are effectively operated, incentivised and clearly accompanied by benefits for certified organisations. Otherwise, organisations will be reluctant to invest time and money in obtaining and maintaining GDPR certifications on top of the many other certifications and requirements to which they are already subject.

Required Action/Decision Points

1. No decision points required by Senior Officials
2. No deliberations required by Senior Officials



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS/011

Agenda Item: 1(b)

**Report Data Privacy Sub-Group Meeting,
23 February 2017, Nha Trang, Viet Nam**

Purpose: Consideration
Submitted by: APEC Secretariat



**Data Privacy Sub-Group Meeting
Ho Chi Minh City, Viet Nam
21 August 2017**

**REPORT OF 35th APEC ELECTRONIC COMMERCE STEERING GROUP
DATA PRIVACY SUB-GROUP (ECSG-DPS) MEETING
9:00 am to 6:00pm, 23 February 2017
Liberty Central Hotel
Nha Trang, Viet Nam**

AGENDA #1. INTRODUCTION AND ADMINISTRATION

1. The 35th ECSG-DPS meeting was held on 23 February 2017. The meeting was chaired by Mr Colin Minihan, Australia. The ECSG-DPS meeting was preceded by an informal session held on 22 February 2017. The following member economies and guest organisations were represented at the meeting: Australia; Canada; China; Hong Kong, China; Japan; Korea; Malaysia; Peru; Philippines; Russia; Singapore; Chinese Taipei; Thailand; United States; Viet Nam; APEC E-Commerce Business Alliance (APEC ECBA); Center for Information Policy Leadership (CIPL); International Chamber of Commerce (ICC); Internet Society (ISOC); World Trustmark Alliance (WTA); and World Economic Forum (WEF).

(a) Approval of the Agenda

2. The agenda (2017/SOM1/ECSG/DPS/001) was approved.

(b) 33rd ECSG-DPS Meeting Report

3. The noted and approved the 34th ECSG-DPS Meeting Report (2017/SOM1/ECSG/DPS/002).

(c) DPS Executive Positions

4. The ECSG-DPS Chair noted the following appointments that were endorsed by the ECSG intersessionally:

(i) 2nd Vice Chair: Mr Ahn Kun Young, Director, Consumer Protection Division, Consumer Policy Bureau, Korea Communications Commission (KCC), was elected as the second Vice Chair of the ECSG-DPS from SOM3, 2017. Mr Ahn's term will be for two (2) years and will end at SOM3, 2019; and

(ii) CBPR Joint Oversight Panel (JOP) Position: Mr Ahn Kun Young, Director, Consumer Protection Division, Consumer Policy Bureau, Korea Communications Commission (KCC), was elected as the JOP for a two-year term.

5. The ECSG-DPS Chair noted that he had relinquished his JOP membership since his appointment as the Chair. Notwithstanding, the ECSG-DPS Chair would be available as an alternate JOP member, if necessary, for example, if the JOP is considering the CBPR application of a JOP member economy.

(d) Report from DPS Representative Attending 2016 ICDPPC Meeting

6. Ms Shannon Coe, Chair of the ECSG who participated as the APEC ECSG observer at the 38th International Conference of Data Protection & Privacy Commissioners (ICDPPC) held in Marrakech in October 2016 informed the meeting that she had not represented APEC ECSG but instead represented as the United States representative.

AGENDA #2. CROSS BORDER PRIVACY RULES (CBPR) SYSTEM

(a) Summary of outcomes from 2016 Leaders and Ministers meetings

7. The ECSG-DPS Chair briefed the meeting the outcomes of the 2016 Leaders and Ministers meetings, noting that the Ministers (2016/AMM/JMS) and Leaders (2016/AELM/DEC) have recognised the importance of the APEC CBPR system and supported enhanced cooperation, including through promoting capacity building.

- (b) Report from the Joint Oversight Panel Chair
 - i. Opportunity for Economies to communicate Intent to Participate

8. The **JOP Chair** informed the meeting that the current membership of the JOP comprised the United States, Japan and Korea following members' endorsement of Korea's application. The JOP was currently reviewing three (3) issues. First, the review of the CBPR application from Korea. Second, the US' PRP application. Third, the review of JIPDEC's renewal as an AA for CBPR. The JOP Chair noted that JIPDEC's renewal would be for a period of two years. The JOP Chair also thanked Singapore for its proposal on the AA and noted that the issue was under consideration by the JOP.

9. **Chinese Taipei** announced its intention to join the CBPR system, noting that a task force comprising 15 different ministries and commissions have been set up to review and assess Chinese Taipei's participation in the CBPR system. Chinese Taipei noted that the review is in its preliminary stages. Notwithstanding, capacity building activities have been scheduled for 2017 to consult the relevant stakeholders and businesses. Chinese Taipei has also submitted a proposal for an APEC seminar to be held at the end of the 2017 as part of its domestic outreach and consultation exercise.

10. **Singapore** informed the meeting that it had completed its study on the CBPR and did not identify major gaps between the CBPR and the Singapore Personal Information Protection Act (PDPA). The next step in its assessment for CBPR application is to consult its agencies and businesses to ensure that Singapore can fully operationalise the CBPR before an official intent to participate in the CBPR system is submitted to the JOP.

11. The **Philippines** similarly noted its interest to participate in the CBPR system. Noting that while efforts were focused on developing domestic regulatory capacities, the CBPR system was one of the Philippines' priorities in the global sphere.

- (c) Updates from existing CBPR economy participants

12. The **United States** updated the meeting on the growth of the CBPR system, including an assessment on the suitability of a second AA in the United States. The United States has continued to engage the region to further raise awareness of the CBPR and welcomed requests from interested members. The United States noted that its policy on the CBPR remained unchanged despite the new Administration in place.

13. **Japan** thanked Chinese Taipei, the Philippines and Singapore for indicating their interest to participate in the CBPR system. Japan shared with the meeting there a joint seminar was conducted together with the Department of Commerce, United States and TRUSTe in October 2016. The seminar was attended by more than 200 companies who were trained how to obtain the CBPR certification. Japan granted its first CBPR application in September 2016. Japan noted that JIPDEC had already submitted its application to extend its AA status, and awaiting JOP decision. Lastly, Japan informed that the 16 different competent enforcement ministries in Japan would be merged under one single agency, the newly established Personal Information Protection Commission (PPC), in end May 2017. Japan would be submitting its formal notification to the CPEA shortly. PPC presented an overview of its establishment and its mandate (2017/SOM1/ECSG/DPS/005).

14. **Canada** informed the meeting that Canada was ready to accept applications for AA under the CBPR, and it had published a public interest in January 2017.

15. **Korea** noted that it had submitted its official intent to participate in the CBPR system to the JOP in late 2016 and was awaiting the decision of the JOP. Korea noted that there were two challenges in implementing the CBPR in Korea, viz. (i) ensuring interoperability between the Personal Information Management System (PIMS) and the CBPR and (ii) outreach to companies and encouraging domestic up-take to CBPR certification. Notwithstanding, Korea remained committed to participate in the CBPR.

- (d) Administration and Accountability Study Group (AASG)

16. The United States provided an update of the work of the AASG (2017/SOM1/ECSG/DPS/003). Since August 2016, the AASG had 3 teleconferences, with broad representation, including member economies (Australia, Canada, Korea United States, Japan, the Philippines, and Singapore) and AA.

As outlined in the foundation document, the AASG would focus on three workstreams, viz. (i) staffing and resources; (ii) accountability; and (iii) communications. A terms of reference for the cbprs.org website has been developed with a view of completion by SOM3, 2017 (2017/SOM1/ECSG/DPS/004). The current website is also being maintained. The AASG is also considering issues on increased resources to handle accountability, improving transparency through marking documents, as well as on workshops on CBPR in 2017.

17. The meeting endorsed the terms of reference for cbprs.org Enhancements and the intention to use the existing MYP funds submitted by the Administration and Accountability Study Group (AASG), which will be submitted to ECSG for endorsement.

18. The United States will work with the APEC Secretariat on the proposed re-programming of the MYP to support the enhancement to the cbprs.org website.

(e) Outcomes of CBPR readiness Survey

19. The meeting noted the report of the outcomes of the CPBR readiness survey undertaken by Viet Nam (2017/SOM1/ECSG/DPS/016).

AGENDA #3. UPDATED PRIVACY FRAMEWORK

(a) Updates to the APEC Privacy Framework – next steps

20. The ECSG-DPS Chair informed the meeting that the revised APEC Privacy Framework was endorsed at the end of 2016. In terms of outreach and publicity, the APEC Secretariat informed the meeting that e-publication of the Framework would be preferred, as the APEC Secretariat did not have a separate budget for hardcopy publications. Notwithstanding, the APEC Secretariat could assist in working with interested member economies on a media release and infographics. The ECSG-DPS could also work on developing a fact sheet to accompany the launch of the APEC Privacy Framework 2015. The meeting agreed to undertake intersessional consultations on the proposed launch and media release.

21. Japan noted that it was interested in the work that it was interested ISOC noted, in addition to the launch, members could also refer to the work of the OECD on data breach and privacy management framework for future work.

(b) For discussion: possible areas for future work for DPS

- i. Data Breach Notification – Overview of report on economic impact of data breaches - ISOC

22. The meeting noted ISOC's briefing on the report on economic impact of data breaches (2017/SOM1/ECSG/DPS/015).

AGENDA #4. DPS WORKING GROUP ON DATA PORTABILITY

23. The meeting noted the report from New Zealand on the DPS Study Group on Data Portability (2017/SOM1/ECSG/DPS/006). The meeting endorsed the continuation of the study group, including its study on the impacts for the APEC region of the inclusion of a right to data portability in the EU General Data Protection Regulation due to commence in 2018, and for the working group to submit its report to SOM3, 2017.

AGENDA #5. LSIF-ECSG VIRTUAL WORKING GROUP ON HEALTH DATA RESEARCH

24. The meeting noted the updates from the United States on the ongoing work between the ECSG and the LSIF (2017/SOM1/ECSG/DPS/017). The United States would be updating members regularly on the progress of the work.

AGENDA #6. UPDATE FROM CROSS BORDER PRIVACY ENFORCEMENT ARRANGEMENT ADMINISTRATORS (CPEA)

25. The Federal Trade Commission (FTC), United States, provided an update on the CPEA, reiterating the intention of the CPEAs and the criteria for application. At present, the CPEA had 25 members, noting that Japan would be consolidating its 16 enforcement agencies into a single agency at end May 2017. There was a request from the Philippines to join the CPEA which was pending approval. The FTC shared a recent information sharing in enforcement between Canada, Australia and the United States on the data breach by an online dating website. In terms of future work, the CPEA would be working on the AASG issues identified in implementing the CBPR, viz. creating processes including the website for directing complaints, reviewing coordination mechanisms and false claims enforcement. Work could also comprise information sharing on privacy enforcement experience.

AGENDA #7. APEC PROJECTS

(a) Project Management Update

26. The APEC Secretariat provided an update on APEC projects, including an update on the Multi-Year Project (2017/SOM1/ECSG/DPS/007rev1).

(b) Update on Multi-Year Project – CBPR System Capacity Building and Administrative Support

- i. Status Report from MYP Project Lead – United States
- ii. Next steps

27. The United States briefed the meeting on the status of the MYP, noting the earlier discussions on the proposal to update the cbprs.org website, and ongoing discussions with the APEC Secretariat to re-programme the MYP for 2017. The United States invited interested members to submit their requests for CBPR capacity building.

(c) Chinese Taipei Proposal – Capacity-Building for Compliance with Cross-Border Privacy Rules System in APEC

28. Chinese Taipei briefed the meeting on its proposed concept note on “Capacity-Building for Compliance with Cross-Border Privacy Rules System in APEC” (2017/SOM1/ECSG/DPS/008). Chinese Taipei would undertake intersessional consultations with Russia on the concept note due for submission on 7 March 2017.

(d) Viet Nam Proposal – Framework on Cross-Border E-Commerce Facilitation

29. Viet Nam presented its proposal on “Framework on Cross-Border E-Commerce Facilitation”, emphasizing the importance of this framework as a deliverable for Viet Nam’s APEC 2017 chairmanship. Viet Nam noted the preliminary views provided by the members and that further detailed discussions would take place at the ECSG plenary meeting.

(e) New Projects or Activities - the Chair will invite member economies to submit project proposals or activities

30. The ECSG-DPS Chair invited member economies to submit their proposals and activities intersessionally.

AGENDA #8. UPDATED DATA PRIVACY INDIVIDUAL ACTION PLANS

- (a) Australia to present revised IAP**
- (b) Chair will invite economies to update existing IAPs**

31. Australia briefed the meeting on the revised IAP which takes into account of the new elements in the revised APEC Privacy Framework (2017/SOM1/ECSG/DPS/010), and invited members to update their existing IAPs.

AGENDA #9. DPS 2017 WORK PLAN

- (a) The Chair will lead a discussion on the 2017 Work Plan**
- (b) Discussion and decision on Work Plan**

32. The meeting endorsed the DPS Work Plan 2017 for submission to ECSG for endorsement (2017/SOM1/ECSG/DPS/021).

AGENDA #10. REPORTS FROM SUB-GROUP MEMBER ECONOMIES

Member Economies of the Sub-Group are invited to provide a brief (3 minute) report on relevant data privacy developments

33. The meeting received updates from member economies at Annex A.

AGENDA #11. INFORMATION SHARING ON CROSS-BORDER PRIVACY ISSUES

- (a) Guests are invited to provide a brief report (3 minutes) on relevant data privacy developments:**

34. The meeting received updates from ICC (2017/SOM1/ECSG/DPS/014); ISOC (2017/SOM1/ECSG/DPS/015); CIPL (Annex A); ICDPPC; APPA; GPEN; OECD (2017/SOM1/ECSG/DPS/019).

AGENDA #12. CONCLUSION AND NEXT STEPS FOR THE DATA PRIVACY SUB-GROUP

- (a) For information** – Members will have the opportunity to inform the Sub-Group of any other matters by prior arrangement with the Chair
- (b) For review and decision** – Meeting document access

35. The meeting endorsed the meeting document classification list.

- (c) For information** - The Chair will provide a verbal summary of the meeting that will form the basis for the Chair's report to the ECSG

36. The Chair provided an oral summary of the meeting. The report of the ECSG-DPS to the 35th ECSG Meeting is at Annex B.

* * * * *

UPDATES FROM MEMBER ECONOMIES

(a) China

THE LATEST DEVELOPMENT OF CHINA'S CYBER DATA PROTECTION LEGISLATION

37. China does not have a specific data protection law. However, the relevant rules are scattered in diverse laws, regulations and policies. Nearest, china's top legislator, the National People's Congress has issued the Cybersecurity Law, and E-commerce Law is in the process of legislation. Both laws include the issue of data and privacy protection.

38. The Cybersecurity Law of the People's Republic of China, was approved by the Standing Committee of the National People's Congress on November 7, 2016, and will come into force on June 1, 2017. According to the articles, the law applies to the construction, operation, maintenance and usage of networks, as well as the supervision and management of cybersecurity in China. The law states that its objectives are to safeguard China's cyber security, protect against cyber-attacks, and regulate the use of personal data.

39. Specifically, the law requires network operators to improve protection for personal data, privacy and commercial confidentiality. Network operators must follow the principles of legality, propriety and necessity when they collect and use the personal data. Data collectors must notify data owners of the purpose, manner and scope of data collection and usage. The law also requires network operators to take technical safeguard measures, and other appropriate methods to avoid data leakage or loss. The law requires reporting data breaches to relevant authorities and the notification to affected data owners.

40. On December 27, 2016, the National People's Congress of China released an official draft version of E-Commerce Law . The draft is subject to modification after soliciting public opinions. The scope of the Law includes both domestic e-commerce and cross-border e-commerce, setting specific obligations over the responsibilities of e-commerce entities, safety of trade and service, data and information protection, consumer rights protection, fair competition and etc.

41. The draft encourages the exchange and sharing of data and information to ensure the orderly information flow and reasonable use. It requires that e-commerce entity should take appropriate safeguard measures to protect user's personal information. The Draft emphasizes the importance of personal data protection by specifying the requirements for utilizing data generated in e-commerce activities. Any collection of personal information must be based on the user's consent. Further, upon expiration of a statutory or agreed-upon retention period, an e-commerce entity is required to cease its processing and use of relevant personal information, or delete such information.

(b) Korea

42. One on-line company was accused of having leaked 25 million personal information such as ID, oneway-encrypted password, name, gender, birth date, phone number, cellular phone number, e-mail address, address. It was found that the company was negligent of privacy measures and violated the rules on leakage notification. The company punished with the penalty of about 4.5 billion Korean won, about 4 million U\$.

(c) Russia

43. The Meeting noted the presentation from **Russia** on "Brief Report on the Development of Regulatory Practices in the Field of Personal Data Protection in the Russian Federation" (2017/SOM1/ECSG/DPS/012; 2017/SOM1/ECSG/DPS/013).

(d) Singapore

44. As of 1 October 2016, PDPC has been organisationally restructured from a five member commission headed by a Chairman, to a structure headed by a Commissioner and a Deputy Commissioner. Over the last few months, PDPC has issued a number of new guidelines, for example, on Photography, Video & Audio Recording including drones. PDPC has also published several good practices guides, such as on how to handle access requests, what to pay attention to when building websites with respect to responsible handling of personal data, and how to prevent accidental disclosure when processing and sending personal data. We are in the process of reviewing the Personal Data Protection Act (PDPA) to ensure its continued relevance with evolving technology. Some of the issues being considered under the Act Review include alternatives to consent, mandatory data breach notification, and providing binding guidance. Our recent industry survey in 2016 showed that 80% of the organizations surveyed were aware of the PDPA and 70% said that they have put in place policies and measures to comply with the PDPA. While general awareness is high, there are some sectors with lower rates of awareness, such as the retail and manufacturing sectors. Hence, we will concentrate our outreach efforts on some of these sectors.

(e) Thailand

45. Thailand would like to update legal development in Thailand regarding privacy and digital economy. Last year on December (2016) we just passed "the Digital Economy law", in order to transform the country into a digital society and use of technologies in order to develop infrastructure, innovation and human capital. The draft of Data Protection law is part of the package of digital economy legislations since it would provide guarantee of the data protection and ensure people trust and confidence in online transactions. With respect to the updated APEC Privacy Framework, the draft of Data Protection law also includes "Data Breach notification" and "self-regulation" that will provide the guidance for the private sectors in implementation of the law.

46. After discussions with the private sectors in particular those from financial sectors, we have set up the working group under the Ministry of Digital Economy and Society to review the draft of Data Protection law in order to mitigate the barriers faced by the private sectors especially SME while its principle still maintains in digital age.

47. Finally, back to the survey of CBPR readiness from Vietnam, even Thailand has not yet participated in CBPR system, we attach the importance of CBPR system. We believe that participation CBPR system will be beneficial to both large companies and SME in Thailand when they manage free flow of data across the countries.

(f) Chinese Taipei

48. The Ministry of Economic Affairs (MOEA) supports and protects personal information through two main mechanisms: one is providing counseling to assist online retailers in establishing a personal data management system and enhancing information security; the other one is to implement administrative inspections for enterprises which are suspected of data breach.

49. There are three steps of administrative inspections, including on-site visit, diagnosis and administrative inspection. This year, a total of 24 cases were examined, and 70% of them were significantly improved.

50. In the future, Chinese Taipei will continue to assist EC industry in protecting personal data and will oversee its crime prevention and security measures against data breach.

(g) United States

51. There have been a number of important privacy related developments since the last meeting in August.

Law Enforcement

52. On the law enforcement front, the Commission has brought several cases that involving privacy issues, including three new false CBPR claim cases and two new actions involving the IoT.

False APEC Claims

- First, the Commission charged three businesses with violating the Federal Trade Commission Act by deceptively claiming participation in the APEC CBPR system. Two of the companies provided security software and the third marketed an app that enabled private messaging. In addition, one of the companies also falsely claimed that the US Accountability Agent TRUSTe had certified its practices.
- The Commission has obtained orders, which are currently subject to public comment, against each company that prohibit them from misrepresenting their participation in any privacy or security program. The FTC has now brought four false CBPR claim cases. Like its numerous false US/EU and US/Swiss Safe Harbors cases, these three new actions illustrate the FTC's continued commitment to preserving the integrity of programs like the APEC CBPR system.

VIZIO

- Earlier this month, in an important IoT case, the FTC settled its charges against VIZIO, one of the world's largest manufacturers and sellers of Internet-connected "smart" televisions. The Commission, along with the New Jersey Attorney General, alleged that software on the VIZIO TVs collected viewing data of 11 million consumers without the consumers' knowledge or consent. The Commission's settlement requires the company to prominently disclose and obtain affirmative express consent from consumers for its data collection and sharing practices and to delete the collected view data. It also requires the company to pay 2 million in consumer redress.

D-Link

- Finally, in January, the Commission filed a lawsuit challenging the security practices of D-Link a global manufacturer of computer networking equipment and other connected devices. The complaint alleges the company misrepresented its security measures and failed to take reasonable steps to ensure its connected products did not subject consumers to privacy risks. The case is currently pending in US Federal District Court in California.

Workshops and Reports

- On the policy front, the FTC hosted a public workshop on the privacy implications of Internet connected Televisions as well as a workshop on the latest research and trends related to consumer privacy and data security.
- In addition, last month the Commission released a staff report on Cross Device Tracking, which describes the technology used to track consumers across multiple Internet-connected devices and makes recommendations on best practices (transparency, choice, security, and sensitive data).

- Transcripts of the workshops and the Report are available on the FTC's website at FTC.gov.

CIPL

53. In 2017, the Centre for Information Policy Leadership (CIPL), a global privacy policy think tank, will continue with its multi-year, multi-stakeholder implementation project concerning the EU General Data Protection Regulation (GDPR). This project intends to facilitate the consistent interpretation and implementation of the GDPR through workshops, white papers, webinars, and engagement with EU DPAs, the Commission and government ministries, as well as other means. In addition, the GDPR implementation project is designed to allow participating private sector organizations to benchmark and exchange experiences with respect to key GDPR implementation issues and challenges. CIPL also continues to work on the governance of global data flows and cross-border data transfers. In the Asia-Pacific region, CIPL is particularly engaged in supporting the implementation of the APEC Cross-Border Privacy Rules system and the work on interoperability between the CBPR and EU data transfer mechanisms. Finally, CIPL continues its work on organizational accountability, privacy risk assessments and the risk-based approach to privacy, user-centric transparency and grounds for data processing, such as consent and alternatives consent, particularly as these issues relate to enabling the modern data economy and innovation, while also protecting the privacy of personal data.

- END -

ECSG-DPS REPORT TO THE 35TH ECSG MEETING

- **Endorsed** the report of the DPS Chair, including:
 - o Leadership Positions of the DPS
 - Endorsed Mr AHN Mr Ahn Kun Young as the second Vice Chair of the ECSG-DPS. Mr Ahn's term will be from SOM3, 2017 – SOM3, 2019 – Agenda #1(c)(ii)
 - o Joint Oversight Panel (JOP) Member
 - Endorsed Mr AHN Mr Ahn Kun Young as the third member of the JOP. Mr Ahn's term will be from SOM1, 2017 – SOM1, 2019 – Agenda #1(c)(ii)
 - o Cross Border Privacy Rules (CBPR) System:
 - Noted:
 - The JOP's ongoing review of Korea's application to participate in the CBPR;
 - Noted that the Philippines, Singapore, and Chinese Taipei are at different stages of consideration to participate in the CBPR;
 - Development of communications plan for CBPR
 - Endorsed:
 - the terms of reference for CBPRS.org Enhancements and the intention to use the existing MYP funds submitted by the Administration and Accountability Study Group (AASG); submitted to ECSG for endorsement
 - o Study Group on Data Portability
 - Noted the report of the working group
 - Endorsed the continuation of the study group, including its study on the impacts for the APEC region of the inclusion of a right to data portability in the EU General Data Protection Regulation due to commence in 2018, and for the working group to submit its report to SOM3
 - o DPS Work Plan 2017
 - Submitted to ECSG for endorsement.
- **Agreed to** undertake the following intersessional work:-
 - o APEC Privacy Framework:
 - Launch & Communications: DPS Chair and interested member economies to work with the APEC Secretariat on the proposed launch of the revised APEC Privacy Framework, including work on new release, fact sheet, infographics, and publication.
 - Future Work: Continue work on information sharing on breach notification, privacy management programme, and explore collaboration of collaboration with OECD on developing privacy metrics.
 - o APEC Projects:
 - Chinese Taipei's "Capacity-Building for Compliance with Cross-Border Privacy Rules System in APEC": Chinese Taipei to undertake intersessional consultations with Russia on the concept note due for submission on 7 March 2017.
 - Multi-Year Project (MYP): The United States, as the Project Overseer, to work with the APEC Secretariat on the proposed re-programming and work plan for 2017 .
- **Noted** the following reports received at the DPS:
 - o Updates from existing CBPR economy participants – Canada, Japan, and the United States – Agenda 2(c)
 - o Summary of the Work of the Administration and Accountability Study Group (AASG) – Agenda 2(b) and 2(e)
 - o Viet Nam's report on the Outcomes of the Survey on CBPR Readiness in 2016-2017 – Agenda 2(e)
 - o ISOC on its 2016 Global Internet Report focusing on data breaches – Agenda #3(b)(i))
 - o Status Report from the Study Group on Data Portability – Agenda #4
 - o LSIF-ECSG Virtual Working Group's updates on the joint project – Agenda #5
 - o Update from Cross Border Privacy Enforcement Arrangement (CPEA) Administrators, including the ongoing consideration of the Philippines' intention to participate in the CPEA –Agenda #6
 - o APEC Secretariat's Project Management Update – Agenda #7(a)

- o Status Report from MYP Project Lead, United States – Agenda #7(b)
- o Viet Nam's Proposal "Framework on Cross-Border E-Commerce Facilitation" – Agenda 7(d)
- o Australia's revised Data Privacy Individual Action Plan (IAP) – Agenda 8(a)
- o Member Economies' updates on their respective data privacy developments: Australia; Canada, China; Japan; Korea; Malaysia; the Philippines; Russia; Singapore; Chinese Taipei; Thailand; and Viet Nam – Agenda #10
- o Guest Organisations Updates: ICC; ISOC; CIPL; ICDPPC; APPA; GPEN; OECD – Agenda #11

- END -



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS/012

Agenda Item: 9(a)

**Global Industry Calls for Rapid and Ambitious
Expansion of Participation in the APEC Cross-
Border Privacy Rules System**

Purpose: Information
Submitted by: ITI



**Data Privacy Sub-Group Meeting
Ho Chi Minh City, Viet Nam
21 August 2017**



Global Industry Calls for Rapid and Ambitious Expansion of Participation in the APEC Cross-Border Privacy Rules System

August 17, 2017

Industry associations representing companies from around the world strongly support the Asia Pacific Economic Cooperation (APEC) forum’s work to expand business and economy participation in APEC’s Cross Border Privacy Rules system (CBPRs)¹. We call on the APEC member economies that have not already done so to commit to joining the CBPRs by the November 2017 meeting of APEC Leaders in Da Nang, Vietnam. We also encourage those economies to identify any concrete steps they would take to join.

Since the APEC Leaders meeting in November 2016, the number of member economies participating in the CBPRs has increased to five.² Three additional member economies³ have indicated that they are taking steps to participate. This progress reaffirms both APEC’s recognition of the importance of data flows to trade and investment in the region and its commitment to building bridges between national privacy regimes.

The CBPRs signal to governments in the Asia-Pacific and in other parts of the world that cooperation between like-minded economies delivers high-standard privacy and data protections that facilitate cross-border data flows. We see great potential for the CBPRs to serve as the foundation for a global system of interoperable and robust privacy protection.

Our associations will work with APEC member economies to raise awareness with officials and stakeholders on the benefits of CBPRs. We will do our part to increase the participation of businesses and economies in the CBPRs and help APEC set the global standard for protecting privacy and promoting trust in cross-border data flows.

¹ The CBPRs are based on the internationally respected APEC Privacy Framework and have been endorsed by APEC Leaders since 2011. They are a uniquely interoperable, enforceable, and high-standard privacy code of conduct that facilitates cross-border trade of goods and services and ensures that strong privacy protections will follow personal information across the Asia-Pacific region. By creating a certification system that bridges the privacy regimes of each participating economy in a cost-effective and scalable way, the CBPRs allow participating companies to focus their time and resources on innovating, serving customers, and pursuing their business objectives. For additional information, please see <http://www.cbprs.org/>.

² Canada, Japan, the Republic of Korea, Mexico, and the United States.

³ Philippines, Singapore, and Chinese Taipei.



The associations represented by this statement include:

- Asia Internet Coalition (AIC)
- Asia Cloud Computing Association (ACCA)
- Asociación Latinoamericana de Internet (ALAI)
- Asociación Nacional de Empresarios de Colombia (ANDI)
- Australia Information Industry Association (AIIA)
- BSA | The Software Alliance (BSA)
- Computer and Communications Industry Association (CCIA)
- Computing Technology Industry Association (CompTIA)
- Information Technology Association of Canada (ITAC)
- Information Technology Industry Council (ITI)
- International Chamber of Commerce (ICC)
- Internet Association (IA)
- Japan Electronics and Information Technologies Industry Association (JEITA)
- Japan Information Technology Services Industry Association (JISA)
- Keidanren Japan Business Federation
- Korean Association for ICT Promotion (KAIT)
- National Center for APEC (NCAPEEC)
- Papua New Guinea (PNG) Information and Communication Technology (ICT) Cluster
- Taipei Computer Association (TCA)
- Telecommunications Industry Association (TIA)
- Taiwan Electrical and Electronic Manufacturers' Association (TEEMA)
- U.S. – ASEAN Business Council
- U.S. Chamber of Commerce
- U.S. Council for International Business (USCIB)
- United States Information Technology Office (USITO)

12 April 2017



Discussion Paper

**Certifications, Seals and Marks under the GDPR and Their
Roles as Accountability Tools and Cross-Border Data Transfer
Mechanisms**

Centre for Information Policy Leadership GDPR Implementation Project
April 2017

CIPL's TOP TEN MESSAGES ON GDPR CERTIFICATIONS

1. Certification should be available for a product, system, service, particular process or an entire privacy program.
2. There is a preference for a common EU GDPR baseline certification for all contexts and sectors, which can be differentiated in its application by different certification bodies during the certification process.
3. The Commission and/or the EDPB, in collaboration with certification bodies and industry, should develop the minimum elements of this common EU GDPR baseline certification, which may be used directly, or to which specific other sectoral or national GDPR certifications should be mapped.
4. The differentiated application of this common EU certification to specific sectors may be informed by sector-specific codes of conduct.
5. Overlap and proliferation of certifications should be avoided so as to not create consumer/stakeholder confusion or make it less attractive for organisations seeking certification.
6. Certifications must be adaptable to different contexts, scalable to the size of company and nature of the processing, and affordable.
7. GDPR certifications must be consistent with and take into account other certification schemes with which they need to be able to interact and/or be as much interoperable as possible, such as ISO/IEC Standards, EU-US Privacy Shield, APEC CBPR and the Japan Privacy Mark.
8. Developing a common EU-wide GDPR certification for purposes of data transfers pursuant to Article 46(2)(f) should be a priority for the Commission and/or the EDPB.
9. Organisations should be able to leverage their BCR approvals to receive or streamline certification under an EU GDPR certification.
10. DPAs should incentivise and publicly affirm certifications as a recognised means to demonstrate GDPR compliance, and a mitigation in case of enforcement, subject to the possibility of review of specific instances of non-compliance.

1. INTRODUCTION

1.1 Certifications, seals and marks under the GDPR as promising instruments for data protection

Certifications, seals and marks have the potential to play a significant role in enabling companies to achieve and demonstrate organisational accountability and, more specifically, GDPR compliance for some or all of their services, products or activities. The capability of certifications to provide a comprehensive GDPR compliance structure will be particularly useful for SMEs. For large and multinational companies, certifications may, in addition, facilitate business arrangements with business partners and service providers.

However, certifications must not be made mandatory, but should be treated only as one of many optional tools for companies. There must be no inference of non-compliance if a company chooses not to obtain certification.

In addition, certifications, seals and marks can be used as accountable, safe and efficient cross-border data transfer mechanisms under the GDPR, provided they are coupled with binding and enforceable commitments, including with regard to data subject rights. Finally, there is potential for creating interoperability with other legal regimes, as well as with similar certifications, seals and marks in other regions or in other policy domains.

These instruments present real benefits for all stakeholders, including DPAs and, most importantly, individuals. They have the potential to assist organisations in delivering better compliance and more effective protection for individuals given that certified organisations will have made a conscious effort to become GDPR compliant and will have been reviewed by a third party in that respect.

This is why CIPL generally supports the certifications, seals and marks in the GDPR. However, it is crucial that certifications are effectively operated, incentivised and clearly accompanied by benefits for certified organisations. Otherwise, organisations will be reluctant to invest time and money in obtaining and maintaining GDPR certifications on top of the many other certifications and requirements to which they are already subject.

1.2 The CIPL GDPR Project

This paper is produced by the Centre for Information Policy Leadership at Hunton & Williams (CIPL) as part of its project (CIPL GDPR Project) on the consistent interpretation and implementation of the GDPR.

The CIPL GDPR Project—a multiyear-long project launched in March 2016—aims to establish a forum for dialogue amongst industry representatives, the EU DPAs, the European Data Protection Supervisor, the European Commission, the ministries of the member states and academics on the consistent interpretation and implementation of the GDPR through a series of workshops, webinars, white papers and comments.

CIPL aims to provide input to the Article 29 Working Party (WP29) on a number of priority areas, identified in CIPL's GDPR Project work plans for 2016 and 2017.¹ This is the fourth white paper in this series, following earlier CIPL papers on DPO, Risk, and OSS and Lead Authority.²

1.3 CIPL's Certifications Paper

In this paper, CIPL aims to provide the WP29, the EU Commission and data privacy practitioners with input on certifications, seals and marks under the GDPR and the roles of these instruments as accountability tools and cross-border data transfer mechanisms.

The paper intends to facilitate the development of certifications, seals and marks under the GDPR³ in a way that is pragmatic and benefits all stakeholders.⁴

CIPL notes that there are both similarities and differences between certifications and approved codes of conduct under the GDPR. Although the synergies between both tools must be identified, CIPL will address codes of conduct separately, at a later stage.

2. BENEFITS OF CERTIFICATIONS

Adherence to approved certification mechanisms under Article 42 GDPR may be used as an element in demonstrating compliance with the GDPR obligations of the controller and processor. Moreover, certification mechanisms have the potential to significantly contribute to effective and efficient privacy protection for individuals in a globalised world. They should evolve into real bridges between different legal regimes and accountability frameworks.

Specifically, CIPL has identified the following benefits of certifications to key stakeholders—individuals, organisations, DPAs and the overall digital ecosystem:

2.1 Benefits for individuals

Certifications carry tangible benefits for individuals.

- **Create trust.** Certifications have the potential of increasing individuals' trust and confidence in a certified organisation's handling of their personal data. This in turn may result in individuals'

¹ See

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_work_plan_17_march_2017.pdf

² See

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_gdpr_dpo_paper_17_november_2016.pdf;

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_the_gdpr_one-stop-shop_30_november_2016.pdf;

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf

³ See Appendixes I and II for a summary of the GDPR certification provisions.

⁴ In this paper, we will use the term "certifications" to encompass seals and marks (without foreclosing a discussion about whether there can be differences between these three concepts).

wanting to engage more with a certified organisation and participating in the digital economy more freely.

- **Greater transparency.** Certification ensures better transparency of processing practices of the organisation, making it easier for individuals to understand and assess relevant data practices and their merits.
- **Effective privacy protection.** Individuals may regard certification as a demonstration of commitment to and compliance with effective and rigorous data protection and complaint resolution practices. Adherence to certification mechanisms by organisations ultimately may deliver better compliance and outcomes for individuals, with their data's being more effectively protected.

2.2 Benefits for Certified Organisations

If implemented effectively, certifications may convey a number of key benefits to organisations.

- **Demonstrate accountability and compliance.** Certification is an element of demonstrating GDPR compliance and accountability.⁵ This is an internal benefit vis-à-vis management, the board and shareholders. It also benefits an organisation externally in its relationships with DPAs, individuals, clients and business partners. It builds confidence and trust in the organisation with these external stakeholders, as well as with the wider public.
- **Operationalising compliance.** Certifications translate high-level GDPR requirements into operational compliance steps that are closely tailored by subject-matter experts to the organisation and their privacy management programs. This may result in more relevant, fit-for-purpose and effective privacy and data management programs.
- **Scalable for SMEs and start-ups.** For SMEs and start-ups, well-conceived and properly implemented certifications can serve as scalable and at the same time comprehensive compliance mechanisms that make relevant GDPR accountability obligations less burdensome, less costly and easier to implement, in particular for organisations that do not yet have fully developed privacy management programs or their own internal privacy experts and staff. The third-party certification body will have the expertise and the obligation to ensure that the certifying organisation has policies and processes in place that comply with the GDPR. This improves both organisational compliance and privacy protections for individuals.
- **B2B due diligence and risk management.** In B2B relationships, certification may efficiently demonstrate GDPR compliance and accountability on the part of the processor or service provider. For the same reason, it may also serve as an effective risk-management tool in B2B relationships by lowering the risk profile of the certified processors or providers, thereby directly lowering the risk level of the involved processing as well as the need for DPIAs and/or prior consultations with DPAs.

⁵ Article 24(3) GDPR.

- **Enabling cross-border data transfers.** Certification provides legal certainty to organisations by enabling them to share personal data lawfully outside the EU and across borders, provided that certification is coupled with binding and enforceable commitments.
- **Interoperable and global reach.** The effect of a GDPR certification as a cross-border transfer mechanism could be even stronger when the certification is made interoperable with other, similar mechanisms, thereby extending the certification's geographic coverage and reach. Examples of systems with which GDPR certification could be made interoperable include the ISO Cloud Privacy and Security Standard, the Japan Privacy Mark and the APEC Cross-Border Privacy Rules (CBPR).
- **Mitigating factor in DPA oversight and enforcement.** In addition to serving as demonstration of compliance in the context of audits or other inquiries by DPAs, certification is potentially a mitigating factor in connection with GDPR enforcement and the determination of sanctions.

2.3 Benefits for DPAs

Certification mechanisms have the potential for supporting the oversight missions of DPAs and making it possible for them to leverage their scarce resources more effectively.

- **Reduce oversight workload.** Where certification bodies take on and share the burdens of supervision and oversight with the DPAs, this has the potential of reducing the DPAs' workload.
- **Compliance.** Certifications may result in improved outcomes and more effective compliance on the ground due to the certification process, therefore reducing the enforcement burdens of DPAs.
- **Reduce complaint handling.** Because certifications may include complaint handling and dispute resolution mechanisms, they can help reduce DPAs' involvement in resolving individual complaints. This aspect of certifications will be important in practice, given that the GDPR gives DPAs a significant complaint-handling role.
- **Transparency.** Certification will require organisations to disclose their data practices in a transparent and organised fashion vis-à-vis the certification bodies and ultimately DPAs. This will make it easier for DPAs to properly assess these practices as well as possible violations of the GDPR. This, in turn, may drive down the costs and burdens of enforcement actions, both for DPAs and organisations.

2.4 Benefits for the Ecosystem and for Business Partners

The entire business ecosystem, including non-certified businesses, may benefit from certifications.

Because certifications signal a certain level of data protection and the presumption of GDPR compliance, certifications could streamline and shorten B2B due diligence and risk assessment processes between certified and non-certified organisations seeking qualified and trusted business partners in the digital ecosystem. This could lead to a greater speed of doing business and avoid protracted negotiations about privacy and security, benefiting business beyond just certified companies.

3. KEY POINTS AND RECOMMENDATIONS

3.1 GDPR Certification as an Opportunity

Certifications have significant potential as accountability and compliance mechanisms and for delivering privacy protection to individuals. For this potential to be realised, the following conditions must be fulfilled:

- **Promote benefits and incentivise businesses to adopt certifications.** Industry must be given the right incentives to take up certification instruments. This requires putting in place a certification process that is efficient and appropriately fast, scalable and affordable for all sizes of organisations. It also may include promoting the benefits of certifications by allowing certified organisations to transfer data outside the EU or to engage in broader data uses consistent with the GDPR and by recognising them as mitigation in enforcement and other interactions with DPAs. Otherwise, organisations will be reluctant to invest time and money in obtaining and maintaining certifications (in addition to the many other certifications to which they are already subject).
- **Certification granted to a company must also be stable and valid for at least three years** to avoid a constant cycle of re-certification at short intervals. The renewal of GDPR certifications after three years should be as easy and efficient as possible.
- **Emphasise features of building trust and a competitive advantage.** Certifications must be helpful and recognisable to individuals. Individuals must have trust in certifications and be able to rely on them in deciding with whom to do business, thereby providing certified companies or processes a competitive advantage vis-à-vis non-certified companies. In addition, certifications must be capable of engendering trust in the B2B context and provide a competitive advantage in that context as well.
- **Avoid one-size-fits-all.** Certifications should be adaptable, scalable to all sizes of companies and the nature of processing, and affordable without deviating from the core elements of the EU-wide GDPR baseline certification (discussed below at 3.3). This includes controllers and processors, large companies as well as SMEs, start-ups, etc. The adaptability and scalability would go to “how” these core elements are applied in the particular context and which elements may or may not be applicable at all.
- **Allow a variety of certifications.** The GDPR does not specify the object of certification, other than “processing operations” (Art. 42(1)) and “products and services” (Recital 100). In CIPL’s view, consistent with the relevant GDPR provisions, the object of a certification can be a product, system or service, a particular process, or an entire privacy program⁶ and information management infrastructure, or the full range of an organisation’s products and services.⁷ Limiting availability of certifications to only products, services or a technical process rather than an entire privacy program would seriously undermine the relevance, usefulness and thus

⁶ Any certification of a privacy management program should be based on, or take into consideration as certification referentials, WP 155 BCR for controllers and WP 195 BCR for processors.

⁷ Although the certification of DPOs has merits and may support the role of DPOs, we take the view that this specific certification falls outside the scope of Article 42 GDPR.

attractiveness of certifications. In any event, what is to be certified must be clearly articulated and distinguishable from non-certified products, processes, services or programs by and within an organisation. Consumer confusion must be avoided. Finally, not all products or services have to be certified at the same time, but different certifications within one organisation might be staggered.

- **Keep certifications technologically neutral.** Certifications should not be linked to any particular technologies, tools or frameworks that are prone to change over time. However, certifications should be technology-aware, in the sense that they take account of the impact of various technologies on personal data protection.
- **Certifications should reflect or be able to accommodate the latest developments.** Certifications should reflect or be able to accommodate up-to-date standards, current expertise and the most recent techniques. To accomplish this, certifications must be flexible enough to allow their application in contexts where technology and business practices evolve.
- **Benefit from existing certifications, including BCR and avoid bureaucratic and slow processes.** Because certification will normally require real effort and investment of resources from companies, it is important to find ways for organisations to benefit from existing certifications that are GDPR compliant, including Binding Corporate Rules (BCR). Companies will not want to start a process of “re-certification” at additional costs, if they have already been certified on the same or similar standards or requirements, but under a different name, or in different legal regimes or in different jurisdictions. Compliance with existing frameworks should be considered and recognised under the GDPR certification scheme. In short, certifications under the GDPR should not lead to another layer of bureaucracy. (See also discussion of BCR in 3.6 below.)
- **Learn lessons from the BCR approval process.** Lessons that need to be learned include, for example, the slow uptake by companies that may be associated with lengthy and costly processes.

3.2 Relationship between certifications, seals and marks

The GDPR does not specify a difference or relationship between certifications, seals and marks.⁸ Indeed, the three concepts are not typically seen as something different but as co-equivalents.

CIPL believes that future work on GDPR certifications, seals or marks should not introduce unwarranted and unnecessary differentiation between these terms. However, it should be explored whether different elements of the certification process can be separated and performed by different actors. Possibly, certain actors could deliver parts of, or intermediate steps towards, a certification, seal or mark that is ultimately issued by a certification body or a DPA.

3.3 The need for one EU baseline certification

To ensure effectiveness and take-up of certifications, CIPL recommends the following:

⁸ Certifications, seals and marks are not equal to icons, a transparency tool provided for in Article 12 GDPR. However, they may have a logo, mark or symbol that signifies them, just like an icon may signify a certain privacy or information management and use practice.

- **Preference for one EU baseline certification for all contexts and sectors, with possible differentiation in its application.** Ideally, there would be one baseline EU-wide certification standard—the “common certification” or “European Data Protection Seal” under Article 43(5) of the GDPR—developed under the lead of the Commission or the EDPB in collaboration with certification bodies and industry.
 - This standard or common certification should contain a comprehensive set of certification criteria that are both sufficiently granular and comprehensive to provide for EU-wide consistency and sufficiently high-level and flexible to allow for sector-, industry- and context-specific adaptation and application by certification bodies.
 - This standard or common certification may subsequently be applied taking account of the specific nature and complexity of the specific certifying company, product, service, process or whatever the object of certification might be. Not all the requirements necessarily come into play with each process or organisation. A less complex process or a smaller company may trigger the application of a more limited number of elements of this baseline certification. For example, a processor’s certification might focus primarily on the data security elements and omit aspects of the certification not relevant to it.
 - As to differentiation in applying this baseline EU-wide certification between industry sectors, specialised certification bodies (or sophisticated, non-specialised certification bodies that have expertise with multiple or all industries) could specify this baseline certification to the needs, practices and circumstances of a particular industry sector. Approved sector-specific codes of conduct could be one mechanism to facilitate the sectoral-application of a baseline certification standard.
 - CIPL believes that creating separate sectoral or national certifications without reference to a general baseline EU-wide certification may be confusing, inefficient and unnecessary. Existence of a general comprehensive certification standard would enable specialised application and adaption of that baseline to specific sectors, such as pharma, advertising, credit referencing, etc.
 - The GDPR does allow national and EU-wide certifications to work in parallel. However, certifications that currently exist in the EU at the national level (or may exist in the future) should be aligned with this common EU-wide GDPR certification, including GDPR certifications that may already be under development in member states.
 - It is paramount to avoid an overlap and proliferation of certifications and seals in the EU (or elsewhere) as this could lead to confusion for all stakeholders, including individuals, and discourage organisations from seeking certification altogether.
 - National certifications should be used only for organisations whose privacy programs, services and products are limited to a single member state. These national certifications should not only be issued in full compliance with Art 42(5), but before they are issued, it should also be ensured that they are consistent with each other and the general EU certification. Otherwise, there will be confusion for individuals and businesses moving and operating across the EU.

- There should be a mechanism for companies that are certified at the member states level to have that certification recognised in additional member states and also at the EU level. The Commission is encouraged to use its powers under Art 43(8) and (9) to set up such a mechanism. The EDPB can also set up mutual recognition process for national certifications.

3.4 Certification and compliance

- **Certification as an element of compliance and presumption of compliance** GDPR certification does not necessarily demonstrate full compliance with the GDPR, but it is one of the elements of demonstrating compliance and accountability. However, this one element⁹ of compliance should be understood as a strong presumption that a certified product, process or an organisation's privacy program is in compliance. Thus, DPAs should publicly affirm and support the notion that certifications will be treated as a recognised and accepted means for demonstrating compliance. This is, of course, without prejudice to the DPAs' power to take action and enforcement against a certified organisation where there is a cause to do so and to review specific instances of possible non-compliance. It is essential for the success of certification that DPAs fully implement, recognise and honour the compliance function of certifications.
- **Certification could also go beyond compliance.** Certification is primarily an instrument for demonstrating GDPR compliance and should not exceed the requirements set forth in the GDPR. However, certification can also be used to show proactive and enhanced accountability above and beyond compliance. For example, consistent with the certification requirements, certified organisations may provide additional choices for individuals where possible and useful.
- **Certification should be a mitigating factor in the contexts of accountability and enforcement.** CIPL emphasises the importance of GDPR certification in the context of compliance and accountability, with focus on the issue of certification as a mitigating factor. DPAs should use the existence of certification as a mitigating factor in enforcement and when determining fines. DPAs should explicitly confirm this impact of certification to ensure better take-up in the marketplace.
- **Certification should be an aggravating factor only in exceptional cases.** If a certified organisation deliberately or with gross negligence chooses to ignore its certification commitments whilst gaining financial benefit from such certification, the certification may serve as an aggravating factor in an enforcement matter, or in establishing a fine.
- **Absence of certification should have no negative effect.** DPAs must make it clear that the absence of a certification should not result in a negative inference with respect to compliance. Having no certification should not be interpreted to mean that an organisation is less likely to be compliant. However, we acknowledge that there may be peer pressure in cases where one organisation in a sector gets certified for its product, service or compliance program. The rest of the market may follow for that reason alone. In addition, individuals may take note of who is certified and who is not.

⁹ Art 24(3) GDPR.

- **Failure in receiving certification should have no negative effect.** Another issue relates to an organisation which applies for but fails to obtain a certification from the certification body or DPA. CIPL believes that being unsuccessful in receiving a certification from a certification body or generally withdrawing from the certification application process should not be reportable to a DPA, nor should it otherwise carry negative inferences with respect to compliance. However, it should be clear that this does not mean that an organisation that failed to certify with one certification body or DPA can then seek certification from another based on the same facts and program. Forum shopping must be avoided.

3.5 GDPR certification in relation to other relevant compliance instruments and frameworks

It is important to clarify the relationship between certification and specific accountability instruments and frameworks. Where possible, existing compliance tools should be integrated in the certification process.

- **Certifications must be consistent and take into account other instruments and frameworks, both within and outside EU.** Certifications based on ISO/IEC Standards, the EU-US Privacy Shield, the APEC CBPR and the Japan Privacy Mark are examples of other systems and frameworks having particular importance in this context. We must avoid unnecessary proliferation of different certification schemes or standards and we should use the GDPR process for creating certifications to harmonise, consolidate and make interoperable existing mechanisms, where possible. This requires an assessment of other data protection certifications already existing in the marketplace, in the EU and globally. Ultimately, companies will favour global schemes that are universally recognised.
- **GDPR certifications should have a streamlining effect.** Certifications should be used to streamline risk assessments, due diligence and contracting processes in B2B relationships (including controller/processors relationships). It should be recognised that GDPR certifications could be considered in the context of risk assessments required by the GDPR, whereby a certified company, product or service would have a lower risk profile due to the certification.
- **GDPR certifications should not reinvent the wheel.** The functioning of GDPR certifications should be informed by lessons learned from other third-party privacy and security certification systems, such as the APEC CBPR and those based on ISO/IEC standards.
- **Codes of conduct are different instruments, but have similarities to certifications.** Codes of conduct are approved by the DPAs or provided general validity by the EU Commission. Also, they may include an ability to demonstrate adherence to the code similar to certifications. It should be elaborated how the two instruments relate to each other. It should also be considered how approved sector-specific codes of conduct can leverage certifications to support accountability and GDPR compliance in different sectors.

3.6 Certification and other instruments for data transfer, in particular BCR

CIPL notes that there are significant synergies between GDPR certification and BCR, a key instrument for data transfer which received additional recognition in Article 47 GDPR.

- **BCR are a de facto form of certification.** The two instruments are presented as separate concepts, but, arguably, BCR are a de facto form of certification and it makes sense to elaborate the similarities between the two concepts. BCR-approved companies and their executive leadership all regard their BCR as a de facto certification of their privacy compliance program and a “badge of recognition” by DPAs.
- **Recognise the assessments made in the BCR context.** BCR should be considered a specific type of certification. Thus, it should be explicitly recognised that BCR-approved companies may be given credit for their BCR towards GDPR certification in so far as their BCR meet the relevant certification criteria. (See also bullet on BCR in 3.1 above.)
- **Avoid additional re-certification costs.** The coexistence of the BCR and certifications in the GDPR should not lead to additional costs or investment of resources and efforts. That is why companies that have one of the two, should be able to leverage them for obtaining the other at no unnecessary additional cost.
- **Where a GDPR certification is deemed to provide adequate protection for international transfers, assess the relationship between that certification and other transfer mechanisms.** This assessment should in particular include the relationship with other data transfer mechanisms that work on the basis of a similar certification with which the EU schemes need to interact. This includes the EU/US Privacy Shield and the APEC CBPR.
- **Where a GDPR certification is deemed to provide adequate protection for international transfers, create interoperability with other transfer mechanisms.** CIPL recommends maximising the potential for GDPR certifications as cross-border transfer mechanisms. Thus, at a minimum, the development of a baseline certification standard should be recognised as a data transfer instrument, similar to the benefit offered by the BCR. Further, any new transfer-related certifications should, where possible, avoid creating conflicting requirements with other systems. In that connection, CIPL welcomes the Commission’s interest in “explor[ing] [ways] to promote convergence between BCR under EU law and the Cross Border Privacy Rules developed by the Asia Pacific Economic Cooperation (APEC) as regards both the applicable standards and the application process under each system.”¹⁰ Of course, the same applies to “convergence” efforts between any new EU-based certification or codes and the APEC CBPR. We emphasise that many global companies have a single privacy management program, with all of its essential elements and substantive privacy requirements, that they apply consistently and comprehensively to their processing activities in all countries where they operate. They then leverage this same program to obtain Privacy Shield certification in the US, CBPR in APEC and BCR in Europe, under the respective approval and certification rules.

4. The roles of the various actors and recommendations

The GDPR provides roles to various actors in respect of certification. For instance, the Commission, DPAs and the EDPB all have roles in developing and drafting the standards or criteria for certification, but it is not evident who takes the lead. Also, the GDPR requires the member states, the DPAs, the EDPB and the

¹⁰ Communication from the Commission to the European Parliament and the Council; Exchanging and Protecting Personal Data in a Globalised World, Brussels 10.1.2017, COM (2017) 7 final (emphasis added), available at http://ec.europa.eu/newsroom/document.cfm?doc_id=41157

Commission to encourage the establishment of certification mechanisms. Here, it may be less crucial to lay down who takes the lead, but it would nevertheless be productive if these actors coordinate their efforts and develop a common approach. Regardless of who takes the formal lead, it is crucial that certification bodies and industry stakeholders participate in the development of the certification standards, criteria and mechanisms.

4.1 Member states

- Under the GDPR, (the governments of) member states must “encourage” certifications (Art 42(1)) and must ensure that certification bodies are properly accredited by a DPA or a national accreditation body. They should fulfil these roles under the GDPR in a proactive and consistent manner.
- It is key that member states encourage the certification and accreditation tasks in a coordinated manner, to ensure consistent approaches and avoid discrepancies between the implementation of these mechanisms in the member states.
- The member states’ contributions to the delegated acts and the implementing acts (Art 43(8) and (9)) should be assessed in this perspective.
- At the national level, member states should encourage cooperation between DPAs and organisations in non-data protection domains that have experience in certification. Such cooperation should improve the quality and effectiveness of the GDPR certification processes.

4.2 DPAs

- **DPAs** have wide powers under the GDPR. Inter alia, they have the power to issue, renew and revoke certifications, or, where certifications are issued by certification bodies, the DPAs approve the accreditation criteria for such bodies. They also play a key role in the accreditation of certification bodies, which already exist in many member states.
- DPAs also have the power to disapprove or revoke individual certifications provided by certification bodies “where necessary”. It should be further elaborated how this power will be implemented in a sensible way without introducing a new layer of review in each case. WP29 guidance should develop the appropriate criteria and a process for when and how to exercise this power, based on the notion that this power should be exercised only in exceptional cases.
- Equally, methods must be developed for DPA review of a third party’s certification process, ex ante and/or ex post.
- The accreditation of certification bodies would be a new task for DPAs and does not necessarily fit within their past experiences. It also bears the risk of regulatory capture when the DPAs are required to take enforcement actions against companies, processes, products or services certified by a certification body which the DPA itself has accredited. The risk of regulatory capture is even more pronounced when the DPA itself issues certifications which it must later enforce.

- Thus, CIPL supports a co-regulatory approach with respect to certification, whereby certifications would primarily be provided by third-party certification bodies. (This approach would also help alleviate potential resource issues within the DPAs and potential bottlenecks in the certification process.)

4.3 The EDPB (and WP29)

- The EDPB should agree with the Commission on who is in the best position to initiate an EU baseline certification.
- As mentioned, CIPL believes that, to ensure consistency, there should be one baseline EU-wide GDPR certification that would then be applied by different certification bodies (or DPAs) in different contexts. This baseline certification could be developed by or under the leadership of the EDPB or the Commission. Both the EDPB and the Commission are in the best position to encourage and ensure an EU-wide harmonised approach on certification.
- Before the EDPB will be effectively established, there is a role to play for the WP29. The WP29 should provide guidance at this stage, mainly on the issues addressed in the various parts of this paper. We encourage the WP29 to provide opportunities for the industry to give input before final issuing of guidance. In addition, the WP29 could start leading a process to develop a baseline GDPR certification, with input by relevant stakeholders, including industry.
- As concerns guidance, CIPL expresses a preference for the WP29's providing guidance at this timely stage over guidance by individual DPAs. This guidance should also encompass further defining the role of the lead DPA in EU-wide certifications.

4.4 The Commission

- The Commission should agree with the EDPB on who is in the best position to initiate an EU baseline certification.
- The GDPR gives the Commission a role to pass further implementing and delegating acts.¹¹ CIPL believes these provisions include the authority to develop a baseline EU-wide GDPR certification, and we recommend that either the Commission or the WP29 promptly commence that work, which includes seeking input from stakeholders.
- We recommend that the Commission clarify ambiguous elements of Art 43(8) and (9). More specifically, the Commission should clarify the meaning of (1) "specifying the requirements to be taken into account for the certification mechanisms"; (2) technical standards for certification mechanisms and data protection seals and marks"; and (3) "mechanisms to promote and recognise those certification mechanisms, seals and marks". The Commission should also explain how it seeks to put these provisions into effect.

¹¹ The Commission may adopt delegated acts for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms. (Arts 92 and 43(8)) It may also adopt implementing acts to lay down technical standards for certification mechanisms and data protection seals and marks as well as mechanisms to promote and recognise such mechanisms, seals and marks. (Art 43(8))

- We believe the Commission's role under the GDPR includes ensuring the consistent implementation of certifications and seals in the EU, regardless of whether the Commission or EDPB takes the lead in drafting a baseline GDPR certification.

4.5 Certification bodies

- In general, for efficiency and scalability reasons, CIPL expresses a preference for third-party certification by certification bodies over certification by DPAs (see Art 42(5) GDPR). Certification by certification bodies avoids and alleviates potential resource issues and bottlenecks in the DPAs that could result from widespread use of certifications. It protects the DPAs' functional independence.
- Certification by certification bodies should be set up in a way that ensures an effective and practical participation of the private sector in the certification process. Further work is needed on defining how certification bodies and companies seeking certification will assign the risk between themselves that is associated with a potential DPA disapproval of a certification, such as losing the fee spent on the certification process. It should be established how the risks are divided under those circumstances.

4.6 National accreditation bodies

- National accreditation bodies have the task to accredit certification bodies (the same task is attributed to DPAs). To the extent accreditation is performed by national accreditation bodies as opposed to DPAs, such bodies must ensure that their accreditations of GDPR certification bodies are performed by staff with expertise in data protection and other related matters. This must ensure effective application of the GDPR accreditation criteria.
- The yet-to-be developed accreditation criteria that elaborate on the relevant GDPR requirements in Article 43(2) should be open to public comment and industry input before finalisation by the DPAs and/or the EDPB.

4.7 Private sector organisations

- Private sector organisations, including businesses that might seek certification and potential certification bodies, should have a meaningful role in the drafting and development of GDPR certification schemes and criteria. They are in the best position to advise on the potential impacts and practical implementation challenges that may be associated with specific certification criteria and standards.
- This means there should be a regular consultation with industry by member states, DPAs, the WP29/EDPB, the Commission and non-private sector certification and accreditation bodies, following structured consultation procedures. It also means that private sector organisations should have a proactive approach, taking up signals received in the market.

Appendix I -- Summary of GDPR Certification Provisions

I. Certification in the framework of Article 42 GDPR

Member states, DPAs, the EDPB and the EU Commission must encourage establishment of certifications: (Art 42(1),(3)); see also (57(1)(n); (70)(1)(n)).

- At national and particularly at EU level
- For use by controllers and processors
- Voluntary and available through a transparent process

Controllers and processors may use certifications: (Art 42(1),(2); see also (46(2)(f)); (Articles 24(3) and 28(5))

- As an element to demonstrate compliance with the Regulation
- As an element to demonstrate compliance with the obligations of the controller
- Demonstrate sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation (processor)
- Demonstrate appropriate safeguards in third countries for data transfers; certifications must be coupled with enforceable commitments by the controllers or processors in the third country to apply such safeguards

Certification does not reduce GDPR compliance obligations or prejudice the tasks and powers of the DPAs: (42(4))

- But it is one factor that DPAs must take into account in determining administrative fines—it can be both mitigating and aggravating (83(2)(j)(k))

Certifications are issued by certification bodies or the DPA: (42(5); see also 57(1)(o); 58(1)(c) and (2)(h); 58(3)(f))

- On the basis of criteria approved by the DPA (national) or the EDPB (EU DP seal)
- Last up to three years and are renewable (42(7))
- Can be withdrawn by certification bodies or DPAs, if the certification requirements are not or no longer met
- EDPB maintains a publicly available register of all certifications, seals and marks (42(8)); see also 43(6); 70(1)(o))

To obtain certification from a certification body or DPA, organisations must: (42(6))

- Provide all relevant information about the processing activities they seek to certify
- Provide access to these activities

The Commission's role: (43(8)); (43(9)); see also Art 92, on the exercise of delegation

- May adopt delegated acts to specify the requirements for the certifications (43(8)); see also Art 92, on the exercise of delegation
- May adopt implementing acts laying down technical standards for certifications and mechanisms to promote or recognise certifications

II. Certification bodies in the framework of Article 43 GDPR

Certification bodies issue, renew and withdraw certifications: (43(1))

- Must have an appropriate level of data protection expertise
- DPAs have the power to disapprove or revoke individual certifications provided by certification bodies "where necessary" (See also 58(2)(h))
- Responsible for the assessment leading to certification or withdrawal of certification (43(4))
- Must provide to the competent DPAs the reasons for granting or withdrawing certifications (43(5))

Must be accredited by DPAs and/or national accreditation bodies: (43(1)(a) and (b), 43(3), 43(4); see also 64(1)(c); 57(1)(p); 70(1)(p))

- For a maximum of 5 years
- On the basis of accreditation criteria approved by the DPA or the EDPB
- (Separate requirements in the case of accreditation by a national accreditation body (established according to Regulation 765/2008 (Accreditation Regulation))
- DPAs and EDPB must make public the accreditation criteria for CBs (and certification criteria) (46(6); see also 42(8) and 70(1)(o))
- The DPA or national accreditation body can revoke the accreditation of a CB (43(7))

Conditions for accreditation of CBs: (43(2))

- Demonstrate independence and expertise
- Undertake to respect the approved certification criteria

- Establish procedures for issuing periodic review and withdrawal of certification
- Establish transparent complaint-handling mechanisms
- Demonstrate absence of conflicts of interest

Appendix II -- Schematic Overview Certification Tasks and Actors

GDPR Certification Actors

Member States	DPA's	EDPS	Commission	Certification Bodies	National Accreditation Body	Private Sector Organizations
Encourage Certifications (42(1))	Encourage Certifications (42(1); 57(1)(n))	Encourage Certifications (42(1)); 70(1)(n)	Encourage certifications (42(1))	Issue/renew/withdraw certifications (42(5); 42(7); 43(1))	Accredit Certification Bodies (43(1)(b))	Draft/propose certification criteria and Mechanisms
Ensure that Certification Bodies are accredited (43(1))	Approve accreditation criteria for Certification Bodies (43(1)(b); 43(3); 64(1)(c); 57(1)(p))	Approve accreditation criteria for Certification Bodies (43(3); 64(1)(c); 70(1)(p))	"lay down technical standards for cert. mechs. and mechs. to promote and recognize cert. mechs" (through implementing acts)(43(9)) [Create accreditation criteria for Cert. Bodies?]			Provide input into creation of certification criteria
	Approve certification criteria (42(5); 43(2)(b); 57(1)(n))	Approve certification criteria (42(5); 43(2)(b)); 70(1)(q)(provide opinion to Commission)	Specify requirements for cert. mechs. (through delegated and implementing acts)(43(8)) [Adopt certification criteria?]			Become certified (and attendant tasks, such as providing information and access to Certification Bodies and enter into safeguards commitments with c-b parties) (42(6); 46(2)(f))
	Accredit Certification Bodies (43(1)(a); 43(7); 57(1)(q); 58(3)(e))	Accredit Certification Bodies (70(1)(o))				
	Publicize accreditation criteria and certification criteria (43(6))	Publicize in Register Certification Mechanisms (accredited certification bodies) and certified organizations in third countries (42(8); 43(6); 70(1)(o))				
	Issue/renew/withdraw certifications (42(5); 42(7); 43(1); 57(1)(o); 58(1)(c) and (2)(h)); 58(3)(f))					

GDPR Certification Tasks

Encourage Certifications	Approve accreditation criteria for Certification Bodies	Ensure that Certification Bodies are accredited	Accredit Certification Bodies	Specify requirements for Cert. Mechs and lay down technical standards for Cert. Mechs and promote and recognize Cert Mechs	Draft/Propose Certification Criteria/Mech	Approve/Adopt Certification Criteria/Mechanisms	Issue/renew/withdraw certifications to controllers or processors	Publicize accreditation criteria and certification criteria and mechs
DPAs (42(1); 57(1)(n))	DPAs (43(1)(b); 43(3); 64(1)(c); 57(1)(p))		DPAs (43(1)(a); 43(2); 43(7); 57(1)(q); 58(3)(e))			DPAs (42(5); 43(2)(b); 57(1)(n))	DPAs (42(5); 42(7); 43(1); 57(1)(o); 58(1)(c); 58(2)(b); 58(3)(f))	DPAs (43(6))
EDPB (42(1); 70(1)(n))	EDPB (43(3); 64(1)(c); 70(1)(p))		EDPB (70(1)(o))			EDPB (42(5); 43(2)(b); 70(1)(q) (opinion to Comm.))		EDPB (42(8); 43(6); 70(1)(o))
Member States (42(1))		Member States (43(1))						
Commission (42(1);	Commission (through implementing acts) (43(9)) [?]			Commission (through delegated and implementing acts)(43(8) and (9)) [?]	Commission (through delegated or implementing acts) (43(8) and (9)) [?]	Commission (through delegated or implementing acts) (43(8) and (9) [?]; 92(3) and (5))		
	National Accreditation Bodies under Regulation (EC) No 765/2008 and specified technical rules (43)(3)		National Accreditation Body (43(1)(b))					
							Certification Bodies (with approval/input by the DPA) (42(5); 42(7); 43(1))	
					Private Sector			



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS-EU/001

Agenda Item: 1(a)

Draft Agenda

Purpose: Consideration
Submitted by: DPS Chair



**Data Privacy Sub-Group and European Union
Meeting
Ho Chi Minh City, Viet Nam
22 August 2017**

APEC ECSG DATA PRIVACY SUB-GROUP AND EUROPEAN UNION MEETING
AGENDA

9:00 AM TO 6:00 PM, TUESDAY 22 AUGUST 2017

Rex Hotel
Ho Chi Minh, Viet Nam

1) INTRODUCTION AND WELCOME

- (a) The Chair will request **approval** of the agenda
- (b) **Introduction** of participants

2) INFORMATION SHARING

- (a) Cross-Border Privacy Rules System
- (b) EU General Data Protection Regulation
- (c) Benefits of Interoperability from a Business Perspective
- (d) Industry/ NGO presentations and discussions

3) CBPR AND BINDING CORPORATE RULES (BCR) REFERENTIAL OVERVIEW

4) OPTIONS FOR COLLABORATION

- (a) Interoperability between CBPRs and GDPR
 - i. Certifications
 - ii. Codes of Conduct
- (b) Development of tools to support interoperability
- (c) Other proposals for consideration

5) CROSS-BORDER ENFORCEMENT

- (a) Presentation of CPEA enforcement actions
- (b) Overview of cross-border enforcement provisions under GDPR

6) COMMUNICATIONS ISSUES

- (a) Benefits for individuals and business in understanding cross-border regimes
- (b) Development of joint communications materials
 - i. Release of joint statement in support of interoperability work

7) CONCLUSION AND NEXT STEPS

- (a) Draft of work plan for interoperability work



**Asia-Pacific
Economic Cooperation**

2017/SOM3/ECSG/DPS-EU/002

Agenda Item: 2(d)

Creating Interoperability Between Privacy Program Certifications

Purpose: Information

Submitted by: Centre of Information Policy Leadership




**Data Privacy Sub-Group and European Union
Meeting
Ho Chi Minh City, Viet Nam
22 August 2017**

EXECUTIVE SUMMARY

Certifications, seals and marks can be used as accountable, safe and efficient cross-border data transfer mechanisms. Many of the existing certification and accountability mechanisms in the EU and the APEC region have significant substantive overlap. This enables the development of interoperability between these mechanisms.

Required Action/Decision Points

1. No decision points required by Senior Officials
2. No deliberations required by Senior Officials



Creating Interoperability between Privacy Program Certifications
APEC ECSG Data Privacy Sub-Group and European Union Meeting
 Tuesday, 22 August 2017
 Ho Chi Minh, Vietnam
Markus Heyder
 Vice President & Senior Policy Counselor
 Centre for Information Policy Leadership

Privacy Program Certification Interoperability

Insights from Multi-Certification Projects

Privacy Framework Category	Requirements	EU BCRs (pre-GDPR)	EU BCRs (under GDPR)	APEC CBPRs	Privacy Shield	Referential
Program Management	Governance and Oversight					21
	Training					19
	Complaint Handling					22
	Audit Program / Verification					20
Substantive Privacy and Data Protection Standards	Transparency and Fairness					14, 17
	Purpose Limitation					10
	Data Quality					11
	Security					13, 18
	Individual Rights					15, 16
	Onward Transfer					6, 7, 8
	Basis for Processing Personal Data					12, 13
	Necessity / Proportionality					11
	Privacy by Design and Default					n/a
	National Law Limitations					24
Scope	Relationship to National Law					26
	Geographic Scope					2
	Material Scope					2
Enforceability	Entity List					2
	Purposes of Transfer / Processing					2
	Internally Binding - Entities					3
	Internally Binding - Employees					3
	Third Party Beneficiary Rights					4
	Liability of Applicant Entity					5
	Sufficiency of Applicant Entity Assets					5
	Burden of Proof					5
Access to the BCRs / Policy / Notice					4	
Other	Cooperation Duty					1, 25
	Definitions					9
	Effective Date and Changes					23, 27

Legend

- Green - substantively interoperable / comparable requirements
- Dark Green - more stringent standard
- Light Green - comparable standard, but narrower application / scope
- Yellow - less stringent standard
- Gray - no known requirement

© 2016, TRUSTe All rights reserved.

