Asia-Pacific
Economic Cooperation

Survey on the Readiness for Joining Cross Border Privacy Rules System - CBPRs

Final Report

Electronic Commerce Steering Group

January 2017

APEC Project: M CTI 01 2011T

Produced by

Hang Bui
Viet Nam E-Commerce and Information Technology Agency
Ministry of Industry and Trade
25 Ngo Quyen, Hoan Kiem, Ha Noi, Viet Nam

For
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

APEC#217-CT-01.1

TABLE OF CONTENTS

Research Method

The desk-research method was adopted throughout the whole process of implementing this project with 21 APEC economies.

The questionnaire was circulated to ECSG members and 8 responses were sent back from: Chile; Japan; Korea; Malaysia; the Philippines; Singapore; Thailand; and Viet Nam.

The survey also investigated the privacy regulation of 5 trust-mark providers in APEC region by the responses of questionnaire from Cybersecurity, SOSA, SafeWeb; by desk-research with CNSG and AMIPCI. We excluded TRUSTe and JIPDEC since they have already participated in Cross border Privacy Rules System (CBPRs).

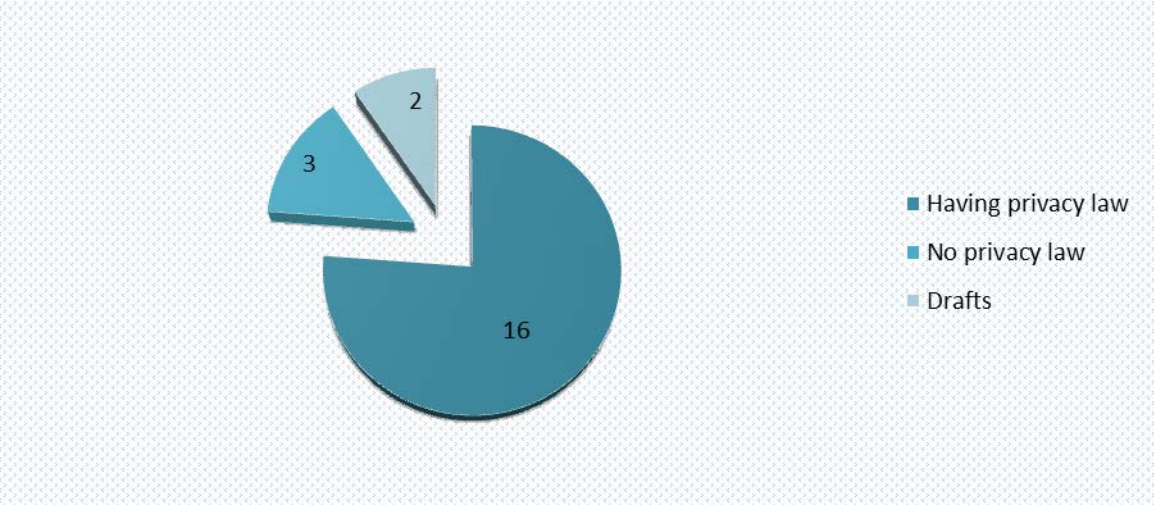
During project, consultations with ECSG official delegate of economies have been done to increase the accuracy of information and to collect data from economies that had not been able to complete the survey questionnaire for some reasons. This has been taken in various stages of the project: conceptualization and implementation.

PART A: THE READINESS OF APEC ECONOMIES WITH CBPRs

I. General information

The questionnaire was designed to survey whether an economy could satisfy basic requirements to participate in APEC CBPRs: the existence of privacy law, enforcement authority on privacy, trust-mark providers; the consistency between privacy legislation with APEC Privacy Framework.[1]

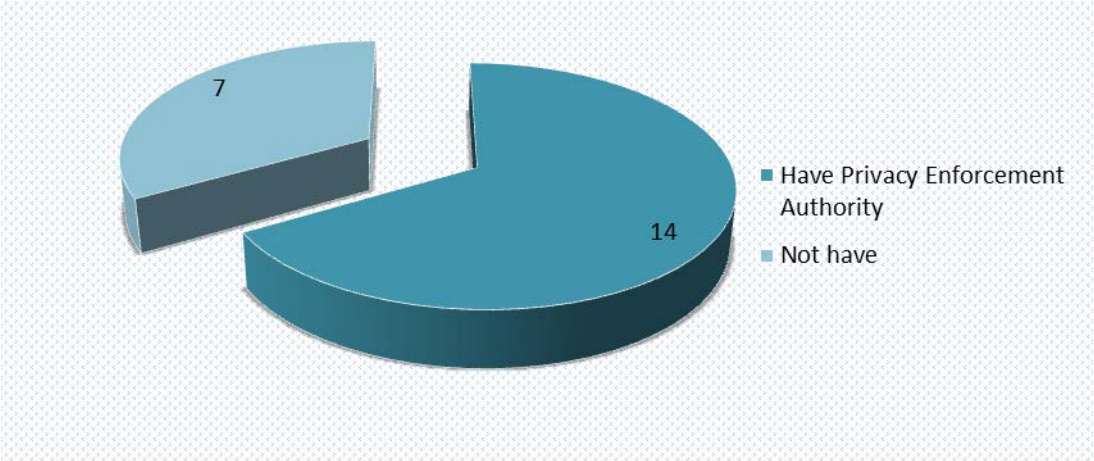
The first requirement that economies should meet to join CBPRs is enacting data privacy law. The result of survey showed that 16 out of 21 APEC Economies have already got a law on privacy for their own.



The following economies have not enacted the single piece of legislation that specifically addresses the personal data protection yet: Brunei Darussalam; China; Indonesia; Papua New Guinea; and Thailand. Recently, China and Thailand released the draft of personal data protection law that might be promulgated soon.

The CBPR Policies, Rules and Guidelines indicate that any economies that want to join this system must have an enforcement authority on privacy. This authority is also required to participate in the Cross-border Privacy Enforcement Arrangement (CPEA).

[1] Further details could be found in 2.2 of the Charter of Cross-border Privacy Rules System: Joint Oversight: http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.pdf



The survey showed that 14 APEC Economies having at least one enforcement authority on privacy. They could be listed as below:

Economies	Name of Privacy Enforcement Authority
Australia	The Office of the Australian Information Commissioner (OAIC)
Canada	The Office of the Privacy Commissioner of Canada (OPCC)
Hong Kong, China	The Office of the Privacy Commissioner for Personal Data, Hong Kong, China (PCPD)
Japan[2]	Ministry of Foreign Affairs of Japan; Ministry of Economy, Trade and Industry of Japan; Ministry of Internal Affairs and Communications of Japan; Ministry of Finance of Japan; Ministry of Justice of Japan; Ministry of Agriculture, Forestry and Fisheries of Japan; Ministry of Land, Infrastructure, Transport and Tourism of Japan; Ministry of Defense of Japan; Ministry of Health, Ministry of Labor and Welfare of Japan; Ministry of Education, Culture, Sports, Science and Technology of Japan; Ministry of Environment of Japan; Cabinet Office of Japan; Consumer Affairs Agency of Japan; Financial Services Agency of Japan; National Police Agency of Japan; Reconstruction Agency of Japan
Korea	Ministry of Interior; Korea Communications Commission

[2] Personal information protection is now under the supervision of the relevant competent Ministers according to the business field. These authorities will be aggregated to the Personal Information Commission (PPC) when, by September 2017, the amended APPI fully take effect – noted by Japan delegate.

Malaysia	Department of Personal Data Protection, Ministry of Communications and Multimedia
Mexico	Federal Institute for Access to Information and Data Protection of Mexico
New Zealand	The New Zealand Office of the Privacy Commissioner (NZOPC)
Peru	National Personal Data Protection Authority, Ministry of Justice
The Philippines	National Privacy Commission
Russia	Federal Service for Supervision of Communications, Information Technologies and Mass Media (Roskomnadzor) - Ministry of Telecom and Mass Communications of the Russian Federation
Singapore	Personal Data Protection Commission, Singapore (PDPC)
United States	The United States Federal Trade Commission (US FTC)
Viet Nam	Ministry of Information and Telecommunication; Ministry of Industry and Trade

Furthermore, CPEA now comes from 9 economies, including[3]:

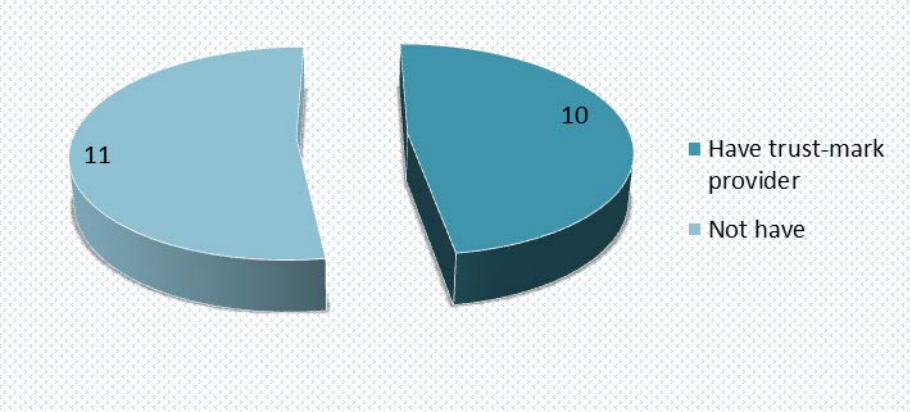
Economies	**Participants**
Australia (1)	The Office of the Australian Information Commissioner (OAIC)
Canada (1)	The Office of the Privacy Commissioner of Canada (OPCC)
Hong Kong, China (1)	The Office of the Privacy Commissioner for Personal Data, Hong Kong, China (PCPD)
Japan (16) (Note: Privacy Protection	Ministry of Foreign Affairs of Japan; Ministry of Economy, Trade and Industry of Japan; Ministry of

[3] http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx

Commission will be chosen to be CPEA of Japan in April 2017)	Internal Affairs and Communications of Japan; Ministry of Finance of Japan; Ministry of Justice of Japan; Ministry of Agriculture, Forestry and Fisheries of Japan; Ministry of Land, Infrastructure, Transport and Tourism of Japan; Ministry of Defense of Japan; Ministry of Health, Labor and Welfare of Japan; Ministry of Education, Culture, Sports, Science and Technology of Japan; Ministry of Environment of Japan; Cabinet Office of Japan; Consumer Affairs Agency of Japan; Financial Services Agency of Japan; National Police Agency of Japan; Reconstruction Agency of Japan
Korea (1)	Korea Communications Commission (KCC)
Mexico (1)	Federal Institute for Access to Information and Data Protection of Mexico
New Zealand (1)	The New Zealand Office of the Privacy Commissioner (NZOPC)
Singapore (1)	Personal Data Protection Commission, Singapore (PDPC)
United States (1)	The United States Federal Trade Commission (US FTC)

The third requirement for joining CBPRs is an APEC Economies must confirm its attention to make use of at least one APEC-recognized Accountability Agent. The Economy do not need to name a specific Accountability Agent at this point, only affirm its intention to use the services of an APEC-recognized Accountability Agent once it has been identified and approved.

According to the survey, 10 APEC member Economies now having at least one trust-mark provider in their locations, comparing to 11 Economies do not have yet.



The name of trust-mark provider in APEC region could be found in the following list:

Economies	Name of trust-mark provider	Website
Australia	AMSRO	http://www.amsro.com.au/
Japan	JIPDEC*	https://english.jipdec.or.jp/
Korea	KISA	www.kisa.or.kr
Malaysia	Cybersecurity	http://www.cybersecurity.my/en/index.html
Mexico	AMIPCI	https://www.amipci.org.mx/es/
Singapore	CNSG	http://www.cnsg.com.sg/
Chinese Taipei	SOSA	
Thailand	DBD Verified	https://www.trustmarkthai.com/
United States	TRUSTe*	https://www.truste.com/
Viet Nam	SafeWeb	http://www.safeweb.vn/

** JIPDEC and TRUSTe are formally recognized as APEC CBPR Accountability Agents*

II. The consistency with APEC Privacy Framework

Survey on the consistency between APEC Privacy Framework and the legal framework on privacy of Economies[4]

Princip	AUS+	BD^	CDA+	CHL*	PRC^	HKC+	INA^	JPN*	ROK*	MAS*	MEX+	NZ+	PNG^	PE+	RP*	RUS^	SGP*	CT+	THA*	USA+	VN*
1	x	-	x	x	-	x	-	x	x	x	x	x	-	x	x	x	x	x	-	x	x
2	x	-	x	x	-	x	-	x	x	x	x	x	-	x	x	x	x	x	-	x	x
3	x	-	x	x	-	x	-	x	x	x	x	x	-	-	x	x	x	x	-	x	x
4	x	-	x	x	-	x	-	x	x	x	x	x	-	x	x		x	x	-	x	x
5	x	-	x	x	-	x	-	x	x	x	x	x	-	-	x	x	x	x	-	x	x
6	x	-	x	x	-	x	-	x	x	x	x	x	-	-	x	x	x	x	-	x	x
7	x	-	x	x	-	x	-	x	x	x	x	x	-	x	x	x	x	x	-	x	x
8	x	-	x	x	-	x	-	x	x	x	x	x	-	x	x	x	x	x	-	x	x
9	x	-	x	-	-	x	-	x	x	x	x	x	-	x	x	x	x	x	-	x	x

x: legal framework on privacy of that Economy consistent with the principle

- : legal framework on privacy of that Economy inconsistent with the principle

blank: unknown status

[4] The information was collected from 3 sources:
- Replies from delegates of Economies (*)
- Data Privacy Individual Action Plan (+)
- Desk research (^)

The table above showed the consistency of privacy legal framework of APEC Economies with the APEC Privacy Framework. According to the answer from delegates, Data Privacy Individual Action Plan and Desk research, there are 13/21 Economies that appear the consistency between their own privacy legislation and the APEC Privacy Framework. 3 of them remain the inconsistency in some principles and 5 are being unable to compare since they have not released their privacy law yet.

The two economies China and Thailand also showed their intention of enacting their law on personal data protection soon. Both China and Thailand published the draft of privacy law last year. In Thailand, the provision of its Personal Information Protection Act is built basing in both APEC Privacy Framework and OECD privacy guideline.

III. Intention of joining CBPRs

According to the questionnaire responses, the consultation with ECSG official delegate of economies and desk-research, the status of 19 APEC economies toward APEC CBPRs are acknowledged. It is easy to see that more than 57% of members showed their interests with the system (4 joined; 2 got plan to join; 6 considering). Only 2 economies replied that they do not have plans to join CBPRs in near future. There are also 5 economies that are unable to participate in the system for now since they have not enacted their data privacy law yet.

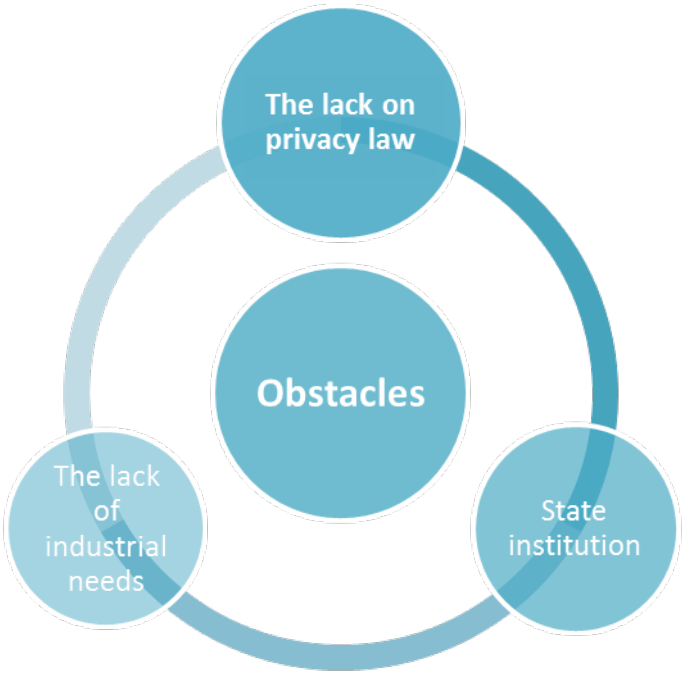
The Philippines estimated the time for participating in CBPRs will possibly before 2019.

Status	Economies
Joined	Canada; Japan; Mexico; United States
Plan to join	Korea, The Philippines
Considering	Australia; Hong Kong, China; Russia; Singapore; Chinese Taipei; Viet Nam
Unable to join	Brunei Darussalam; China; Indonesia; Papua New Guinea; Thailand
No plan to join	Chile; Malaysia

Note: We did not receive the responses from New Zealand and Peru nor were able to collect the information from any other sources.

At the moment, since 5 member economies of APEC are unable to join CBPRs due to the lack of data privacy law, it appears to be the greatest obstacle of joining the system with those economies.

Other barriers had been stated by economies include: the state institution or the lack of industrial needs.



PART B: THE READINESS OF TRUSTMARK PROVIDERS WITH CBPRs

This survey investigates privacy regulations set by trust-mark providers in APEC. The purpose is to make a comprehensive assessment if the regulations are in line with APEC privacy framework. Research methods include questionnaires and desk research.

I. Number of trust-mark providers in APEC

There are several trust-mark providers in APEC as shown in Table 1. However, this survey was conducted among 5 trust-mark providers including CyberSecurity, SOSA, Safeweb, CNSG and AMIPCI.

Economies	Name of trust-mark provider	Website
Australia	AMSRO	http://www.amsro.com.au/
Japan	JIPDEC*	https://english.jipdec.or.jp/
Korea	KISA	www.kisa.or.kr
Malaysia	Cybersecurity	http://www.cybersecurity.my/en/index.html
Mexico	AMIPCI	https://www.amipci.org.mx/es/
Singapore	CNSG	http://www.cnsg.com.sg/
Chinese Taipei	SOSA	
Thailand	DBD Verified	https://www.trustmarkthai.com/
United States	TRUSTe*	https://www.truste.com/
Viet Nam	SafeWeb	http://www.safeweb.vn/

** JIPDEC and TRUSTe are formally recognized as APEC CBPR Accountability Agents*

II. Privacy regulations

The set of questionnaires are applied for the review of processes of trust-mark providers with applicants seeking for trust-mark certification. Questions cover many aspects of privacy regulations including notice, collection limitation, uses of personal information, choice, integrity of personal information, security safeguards, access and correction and accountability.

1. Notice

According to APEC, the Notice Principle in APEC Privacy Framework aims at ensuring that individuals are able to know what information is collected about them and for what purpose it is to be used. When provided with notice, individual can make a more informed decision about interacting with the organizations which collect their personal information[5]. Regarding this matter, all 5 trust-mark providers reported to impose obligation on the applicant to provide individuals the practice and policy that govern their personal information. Concerning the information covered in privacy statement for individual, all 5 trust-mark providers require the purpose of information collecting, and the use and disclosure of personal information to be included. While 3 trust-mark providers obligate the privacy statement to contain information as follows: (1) persons or organizations that may access such information, (2) the identity, address, domicile and other contact information of the personal information controller; (3) method and tools for individuals to access and modify the personal information; and (4) the sharing and personal information to the third party. 2 trust-mark providers ask applicant to introduce (1) method of information collecting and (2) retention and modification policy in privacy statement for individual.

[5] Guide Book on APEC Privacy and Trust-mark

Information	Cybersecurity	SOSA	SafeWeb	CNSG	AMIPCI
Method of information collecting			X	X	
Purpose of information collecting	X	X	X	X	X
Persons or organizations that may access such information	X			X	X
The identity, address, domicile and other contact information of the personal information controller			X	X	X
The use and disclosure of personal information to be included	X	X	X	X	X
Method and tools for individuals to access and modify the personal information	X		X	X	
The sharing and personal information to the third party	X		X		X
Retention and modification policy	X	X			

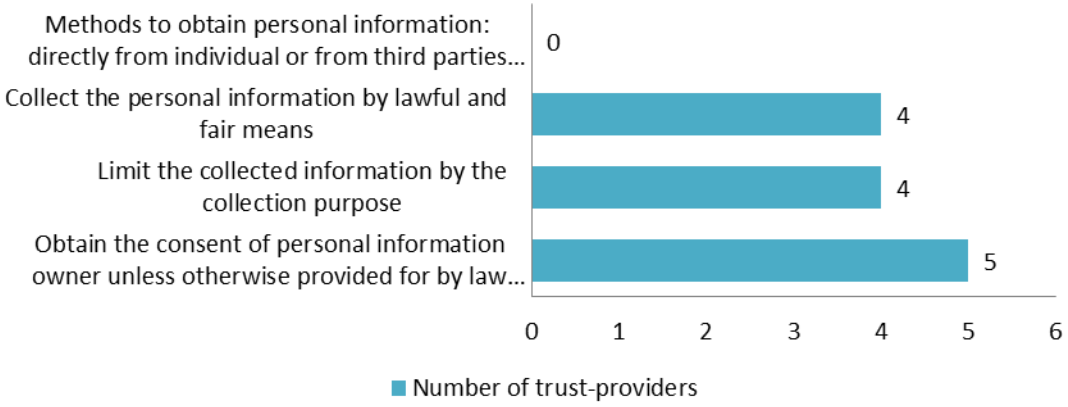
Information included in the privacy statement for individual

(Note: X: Information required by trust-mark provider to include in applicant's privacy statement for individual)

2. Collection limitation

According to APEC privacy framework, the collection of personal information should be limited to information relevant to the purposes of collection and collection methods should be lawful and fair. Concerning this matter, most surveyed trust-mark providers (Cybersecurity, SOSA, SafeWeb, CNSG) stated that their applicants are obligated to obtain the consent of personal information owner unless otherwise provided for by law when collect information; limit the collected information by the collection purpose; and, collect the personal information by lawful and fair means. AMIPCI asked applicant to obtain the consent of personal information owner

only. No trust-mark provider regulates on methods to obtain personal information which may be direct from individual or from third parties on their behalf or other.



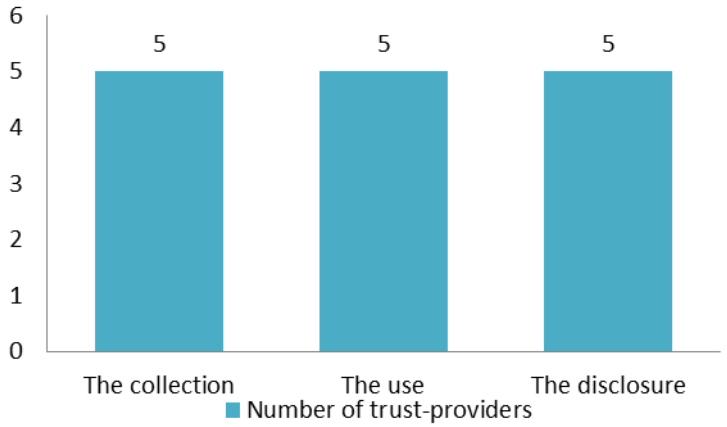
Collection Limitation

3. Use of personal information

APEC stated that personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes, the use, transfer and disclosure of personal information except for some specific circumstances. According to all 5 trust-mark providers, the applicant has to use collected personal information for proper purposes. The applicant also needs to obtain the personal information owner consent for disclosing and or transferring information to a third party.

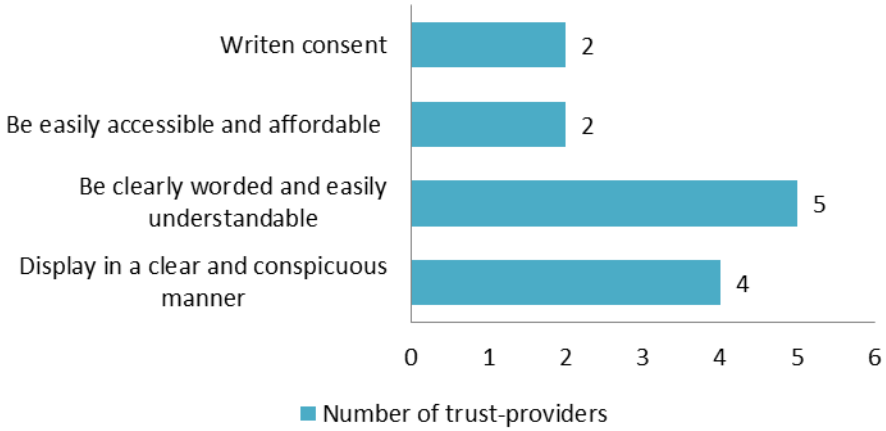
4. Choice

Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. All the 5 trust-mark providers stated that the personal information owners have the right of choice in relation to the collection, the use and the disclosure of their personal information.



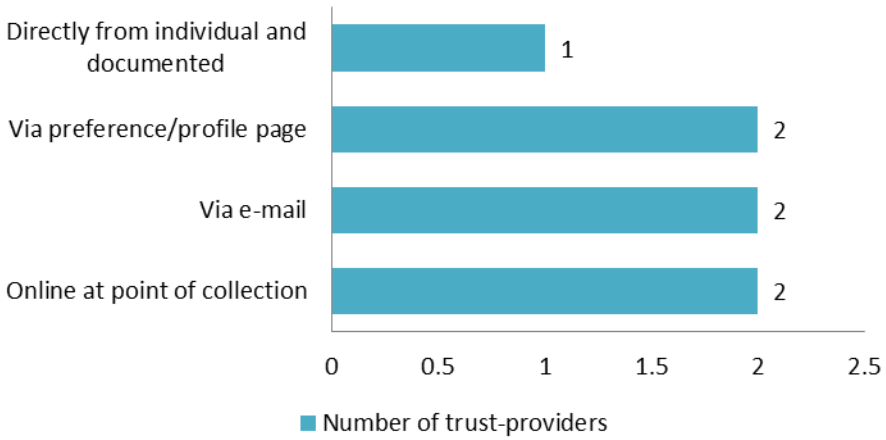
Right of choice for personal information owners in some actions by applicants

According to all 5 trust-mark providers, the information of choice provision is clearly worded and easily understandable. As for 4 out of 5, the choice is displayed in a clear and conspicuous manner. 2 out of 5 reported it is easily accessible and affordable while similar number said it is explicit consent.



How Information of choice provision appear to personal information owners

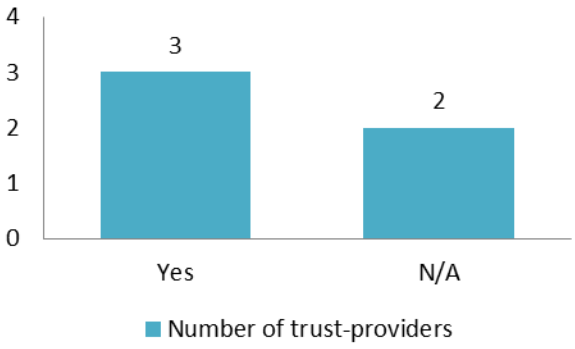
Concerning mechanism for exercising choice, 2 out of 5 trust-mark organizations answered the applicant provides it online, while 2 via preference/profile page, 2 directly from individual and documented and only 1 via e-mail.



Mechanism for exercising choice

5. Integrity of personal information

The questionnaire is designed to check whether or not the applicant is obligated to maintain the accuracy and completeness of records and keep them up to date. 3 out of 5 trust-mark providers asserted that their applicants have to update and correct information by themselves or by other measures, to the extent necessary for the purpose of use. There is no information available concerning 2 trust-mark providers CNSG and AMIPCI.



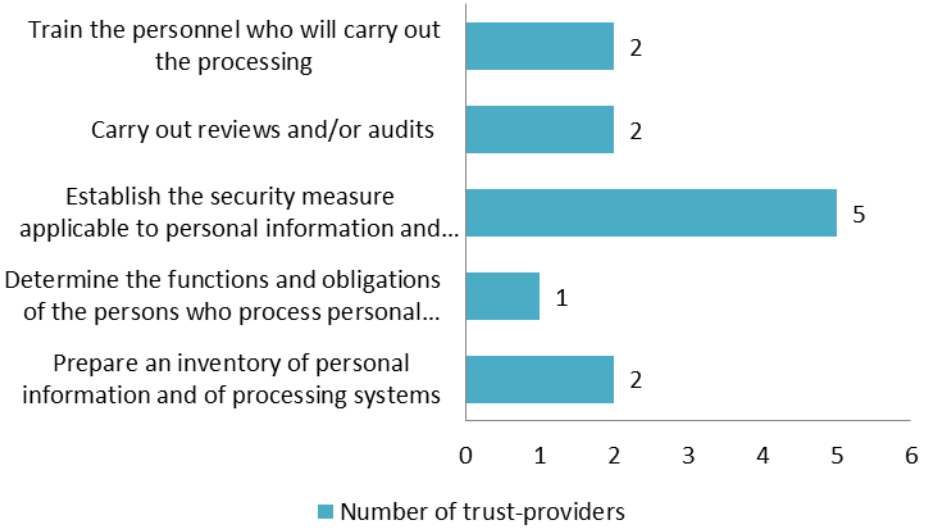
Have applicants had to update and correct information by themselves or by other measures, to the extent necessary for the purpose of use

6. Security safeguards

Security safeguards are expected to protect personal information that a personal information controller hold against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. All 5

trust-mark providers responded that the applicant has to implement an information security policy.

In order to guarantee the security of information, all of them recommend the applicant to establish the security measure applicable to personal information and identify those implemented effectively. While 2 of them ask applicant to prepare an inventory of personal information and of processing systems, 2 demand reviews and/or audits to be carried out and 2 make request for the training of the personnel who will carry out the processing. Only 1 suggests the applicant to determine the functions and obligations of the persons who process personal information. No trust-mark organizations suggest applicant to do following actions: analyze the gap/divine that consists of the difference between existing security measures and those missing, necessary for the protection of personal information; prepare a work plan for the implementation of the missing security measures arising from the analysis of the gap/divine; or, keep a register of storage means of personal information.

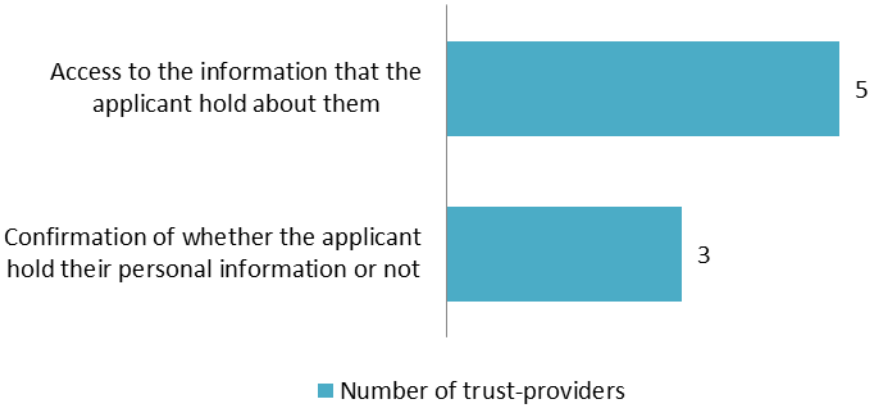


Actions recommended by trust-providers in order to guarantee information security

For all 5 organizations, the applicant is obligated to implement a policy for secure disposal of personal information and measures to detect, prevent and respond to attacks, intrusions, or other security failures. Meanwhile, according to 4 out of 5 organizations there is legal instrument regulating the relationship between the information controller and information processor in order to protect the personal information.

7. Access and Correction

The ability to access and correct personal information is generally regarded as a central aspect of privacy protection. According to the survey, 3 out of 5 trust-mark providers said that the individuals have the right to require the applicant to provide confirmation of whether the applicant hold their personal information or not, while all 5 responded that the individual can access the information that the applicant hold about them. 3 trust-mark organizations with the individuals provided with both 2 rights include SafeWeb, CNSG and AMIPCI.



Information/actions that individuals have right to require applicant to provide

All respondents replied that individuals have the right to request organizations or individuals that store their information in the network environment to correct, complete, update, and/or delete such information.

8. Accountability

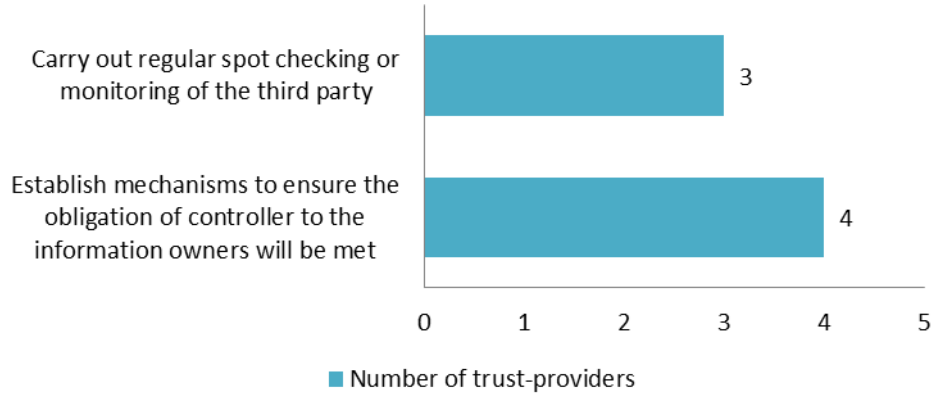
The survey also asks about the applicant's accountability. According to all 5 respondents, the applicant are under obligations to formulate mechanisms for receiving and settling complaints relating to privacy of personal information owners and respond to the complaints of personal information owners in the right amount of time. 4 respondents require applicant to respond to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information. And 3 request for the training for applicant's employees on the privacy policies and procedures including how to respond to privacy-related complaints. Cybersecurity, SafeWeb and CNSG are organizations whose applicant is subject to all 4 above-mentioned actions.

Obligation	Cybersecurity	SOSA	SafeWeb	CNSG	AMIPCI
Formulate mechanisms for receiving and settling complaints relating to privacy of personal information owners	X	X	X	X	X
Respond to the complaints of personal information owners in the right amount of time	X	X	X	X	X
Train employees about the privacy policies and procedures including how to respond to privacy-related complaints	X		X	X	
Respond to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information	X	X	X	X	

Obligation on accountability that trust-mark providers impose on applicant

(Note: x: Obligation imposed by trust-mark provider on applicant)

Efficient and cost effective business models often require information transfers between different types of organization. When transferring information, personal information controllers should ensure that the recipient will protect the information consistently with all principles stated above. Thus, reasonable steps should be taken to ensure the information is protected after it is transferred. In that case, 4 respondents require applicant to establish mechanism to ensure the obligation of controller to the information owners to be met while 3 ask applicant to carry out regular spot checking or monitoring of the third party. SafeWeb and AMIPCI make both above-mentioned compulsory to the applicant.



Actions required when personal information controller authorizes a third party to collect and store personal information

III. Orientation

3 out of 5 trust-mark providers (Cybersecurity, SOSA and SafeWeb) gave answers to the questions relating to APEC Cross-border Privacy Rules (CBPRs). They all knew about the CBPRs and plan to be the Accountability Agent of APEC. However, they did not report about the time for submitting the application for the participation. Also, each trust-mark provider figured out different challenges of joining CBPRs. Cybersecurity highlighted the need to enhance its engagement with the Ministry of Communication and Multimedia, Dept. of Personal Data Protection which is the custodian of the Data Personal Protection Act 2010. SOSA reported there is no consensus among government to be enforcement agency or representative of CBPRs. As for Safeweb, the capacity and social awareness needed to be improved.

ANNEX 1: Privacy questionnaire for designated APEC government delegates

Economy:

Information of delegate:

I. General information

1. Does your economy have a Law on privacy or equivalent legal document regulating on privacy issues?

Yes No *(If NO, please move Part IIa, question 2)*

2. Have you had the agency ready to work as Privacy Enforcement Authority?

A Privacy Enforcement Authority is a public body that is responsible for enforcing an APEC economy's Privacy Law. It will have powers to conduct investigations and/or pursue enforcement proceedings.

Yes No

If YES, please state all their names:

If NO, please state the name of agencies working in privacy issues:

3. Is there any trust-mark provider (known as Accountability Agent) working in your economy?

Yes No

If yes, please provide the following information:

Name:

Website:

II. Orientation

(a) About legal system

1. The purpose of this question is to review the similarity between APEC Privacy Framework and economy's privacy law. Please tick the Principles that your economy's Privacy Law also offers: (multiple choice)

□ Preventing Harm

The purpose of this principle is to prevent misuse of personal information and consequent harm to individuals. Therefore, privacy protection, including self-regulatory efforts, education and awareness campaigns, laws, regulations, organizational control and enforcement mechanisms, should be designed to prevent harm to individuals from the wrongful collection and misuse of their personal information.

□ Notice

The purpose of this principle is to ensure that individuals are able to know what information is collected about them and for what purpose it is to be used. By providing notice, personal information controllers may enable an individual to make a more informed decision about interacting with the organization. One common method of compliance with this principle is for personal information controllers to post notices on their websites.

□ Collection Limitation

The purpose of this principle is to limit collection of information by reference to the purposes for which it is collected. The collection of the information should be relevant to such purposes, and proportionality to the fulfillment of such purposes may be a factor in determining what is relevant. This principle also provides that collection methods must be lawful and fair.

□ Uses of Personal Information

The purpose of this principle is to limit the use of personal information to fulfilling the purposes of collection and other compatible or related purposes. For the purpose of this principle, "uses of personal information" includes the transfer or disclosure of personal information.

□ Choice

The purpose of this principle is to ensure that individuals are provided with choice in relation to collection, use, transfer and disclosure of their personal information. Whether the choice is conveyed electronically, in writing or by other means, notice of such choice should be clearly worded and displayed clearly and conspicuously.

□ Integrity of Personal Information

The purpose of this principle is to recognize that a personal information controller is obliged to maintain the accuracy and completeness of records and keep them up to date.

□ Security Safeguards

The purpose of this principle is to recognize that individuals who entrust their information to another are entitled to expect that their information be protected with reasonable security safeguards.

□ Access and Correction

The purpose of this principle is to include specific conditions for what could be considered reasonable in the provision of access, including conditions related to timing, fees, and the manner and form in which access would be provided.

□ Accountability

When transferring information, personal information controllers should be accountable for ensuring that the recipient will protect the information consistently with these principles when not obtaining consent. Thus, information controllers should take reasonable steps to ensure the information is protected, in accordance with these principles, after it is transferred.

2. If your economy has not had law on privacy yet, then is there any plan of promulgate ones in future?

Yes *(If yes, continue with question 3 – 5)* No *(If no, moving to the section b)*

3. If YES, please provide its name:

4. Will it be a separated law or be a part of another law?

□ A separated law

□ A part of another law, please specify:

5. Will its provisions basing in APEC privacy framework or OECD privacy guideline?

□ APEC

□ OECD

□ Both APEC and OECD

(b) About APEC Cross Border Privacy Rules (CBPRs)

1. Do you have intention of joining CBPRs in future?

If YES, continue with question 2. If NO, move to question 3.

Yes

No

2. If YES, when do you plan to join CBPRs?

…….

3. What are the obstacles of joining CBPRs?

□State institutions

□ The lack of law on privacy

□ The lack of Privacy Enforcement Authority

□ The lack of Accountability Agent

□ Limited capacity

□ Others (specify):

ANNEX 2: Privacy questionnaire for trust-mark provider

I. GENERAL INFORMATION

1. Economy:

2. Name of the trust-mark provider:

3. Contact point:

Name:

Title:

Email:

Phone:

4. The number of trust-mark certifications provided:

5. Do you review the privacy policies of your applicants?

Please only continue with the questionnaire if the answer is YES

Yes No

II. Privacy regulations

These following questions were applied for the review processes of trust-mark providers with applicants, which concern the most about the privacy aspect. (Applicants are websites that seeking trust-mark certification).

Notice

Purpose: *To ensure that individuals understand the applicant's personal information policies, including to whom the personal information may be transferred and the purpose for which the personal information may be used.*

1. Do you have the obligation for the applicants to provide individuals the practice and policy that govern their personal information?

Yes No

2. If YES, which information must include in the privacy statement for individual (multiple choice):

□ Method of information colleting

□ Purpose of information collecting

□ Persons or organizations that may access such information

□ The identity, address, domicile and other contact information of the personal information controller

□ The use and disclosure of personal information

□ Method and tools for individuals to access and modify the personal information

□ The sharing and personal information to the third party

□ Others (specify):

Collection Limitation

Purpose: *Ensuring that collection of information is limited to the specific purposes stated at the time of collection. The collection of the information should be relevant to such purposes, and proportionality to the fulfillment of such proposes may be a factor in determining what is relevant. In all instances, collection methods must be lawful and fair.*

3. Do the applicants have the following obligations?

□ Obtain the consent of personal information owner unless otherwise provided for by law

□ Limit the collected information by the collection purpose

□ Collect the personal information by lawful and fair means

□ Methods to obtain personal information: directly from individual, from third parties on your behalf or others

Uses of Personal Information

Purpose: *Ensuring that the use of personal information is limited to fulfill the specific purposes of collection and other compatible of related purposes. This section covers use, transfer and disclosure of personal information.*

4. Does the applicant have to use the collected personal information for proper purposes?

Yes No

5. What does the applicant need for disclosing and or transferring information to a third party?

□ Obtain the personal information owner consent

□ Compelled by applicable law

Choice

Purpose: *Ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information.*

6. Do the personal information owners have the right of choice in following actions by applicants: (multiple choice)

□ The collection

□ The use

□ The disclosure

7. How must the information of choice provision appear to personal information owners? (multiple choice)

□ Display in a clear and conspicuous manner

□ Be clearly worded and easily understandable

□ Be easily accessible and affordable

□ Others (specify):

8. How do the applicants provide the mechanism for individuals to exercise choice in relation to the use of their personal information?

□ Online at point of collection

□ Via e-mail

□ Via preference/ profile page

□ Via telephone

□ Via post mail

□ Others (specify):

Integrity of Personal Information

Purpose: *Ensuring that the applicant maintains the accuracy and completeness of records and keeps them up to date.*

9. Have the applicants had to update and correct information by themselves or by other measures, to the extent necessary for the purpose of use?

Yes No

Security Safeguards

Purpose: *Ensuring that when individuals entrust their information to an applicant, that applicant will implement reasonable security safeguards to protect individual's information from loss, unauthorized access or disclosure, or other misuses.*

10. Does the applicant have to implement an information security policy?

Yes No

11. If YES, in order to guarantee the security of information, which actions in the following list the applicants are recommended to do:

□ Prepare an inventory of personal information and of processing systems

□ Determine the functions and obligations of the persons who process personal information

□ Have a risk analysis of personal data that entails identifying dangers and estimating the risks to personal information

□ Establish the security measure applicable to personal information and identify those implemented effectively

□ Analyze the gap/divine that consists of the difference between existing security measures and those missing, necessary for the protection of personal information

□ Prepare a work plan for the implementation of the missing security measures arising from the analysis of the gap/divide

□ Carry out reviews and/or audits

□ Train the personnel who will carry out the processing

□ Keep a register of storage means of personal information

□ Others (specify):

12. Does the applicant have the obligation to implement a policy for secure disposal of personal information?

Yes No

13. Does the applicant have to implement measures to detect, prevent, and respond to attacks, intrusions, or other security failures?

Yes No

14. Is there any legal instrument regulating the relationship between the information controller and information processor in order to protect the personal information?

Yes No

Access and Correction

Purpose: *Ensuring that individuals are able to access and correct their information.*

15. Do the individuals have the right to require the applicant to provide:

□ Confirmation of whether the applicant hold their personal information or not

□ Access to the information that the applicant hold about them

16. Do individuals have the right to request organizations or individuals that store their personal information in the network environment to correcting, completing, updating, and/or deleting such information?

Yes No

Accountability

Purpose: *Ensuring that the applicant is accountable for complying with measures that give effect to the other principles stated above.*

17. Does the applicant have the obligation to do the following actions? (multiple choice)

□ Formulate mechanisms for receiving and settling complaints relating to privacy of personal information owners

□ Respond to the complaints of personal information owners in the right amount of time

□ Train employees about the privacy policies and procedures, including how to respond to privacy-related complaints

□ Respond to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information

18. In case the personal information controller authorizes a third party to collect and store personal information, is it required to: (multiple choice)

□ Establish mechanisms to ensure the obligation of controller to the information owners will be met

□ Carry out regular spot checking or monitoring of the third party

III. ORIENTATION

1. Do you know about the APEC Cross Border Privacy Rules (CBPRs)?

If yes, continue with question 2-5

Yes No

2. Do you plan to be the Accountability Agent of APEC?

Yes

No

3. If YES, when will you submit the application?

……

4. If NO, what is the reason you not apply?

…….

5. What are the challenges of joining APEC Cross Border Privacy Rules (CBPRs)?

□ Do not know about the procedure

□ Cannot contact with the government representative

□ Others: …….