APPENDIX 6

APEC CROSS-BORDER PRIVACY RULES (CBPR) SYSTEM – POLICIES, GUIDELINES AND DIRECTORIES

APEC DATA PRIVACY PATHFINDER

CROSS-BORDER PRIVACY RULES SYSTEM

ENDORSEMENT REQUEST

OVERVIEW

The ECSG Data Privacy Sub-Group (the DPS) has completed the projects comprising the Cross-Border Privacy Rules (CBPR) system under the APEC Data Privacy Pathfinder[1]. The purpose of this document is to:

- seek endorsement of the CBPR system, which will recognise the successful completion of the development of the Data Privacy Pathfinder;
- provide a brief overview of the CBPR system and how it satisfies the Pathfinder requirements;
- provide as attachments a package of all documents detailing the elements of the CBPR system (including those previously endorsed); and
- provide a plan for the practical roll-out of the CBPR system between APEC members.

ENDORSEMENT

In considering the documents establishing the CBPR system members should be aware of the following key points:

- a Joint Oversight Panel will be established, comprising member economies nominated by the DPS, to manage the operation of the CBPR system, including undertaking the functions detailed in the Charter of the Joint Oversight Panel;
- the Joint Oversight Panel will report to DPS meetings which will monitor and review the operation of the CBPR system, and report through ECSG to CTI;
- the ECSG will be the forum which economies will notify their intention to participate in the CBPR system; and
- the DPS will conduct a review of the CBPR system two years after commencement to monitor the operation of the system and its implementation by economies (including any proposals for capacity-building programs to assist implementation by economies) and will report to the ECSG on any necessary changes or modifications.

Members should be aware that endorsement of the CBPR system as satisfying the Data Privacy Pathfinder does not mean that an Economy is committed to participate in the CBPR system. Participation is a separate decision to be made by economies as appropriate. The requirements for economies who wish to participate are as follows:

- The Economy informs the Chair of the ECSG that it intends to participate and confirms that it has at least one Privacy Enforcement Authority which participates in the APEC Cross-Border Privacy Enforcement Arrangement (and which has the ability to take enforcement actions under applicable domestic law and regulations that have the effect of protecting personal information consistent with the CBPR program requirements);
- the Economy indicates its intention to make use of at least one APEC recognised relevant Accountability Agent;
- the Economy, after consulting with the Joint Oversight Panel, submits to the Chair of the ECSG an explanation of how the CBPR System program requirements may be enforced in that Economy; and

[1] Subject to final endorsement of two documents at SOM III in San Francisco.

- the Joint Oversight Panel submits to the Chair of the ECSG a report as to how the conditions set out above have been satisfied.

Guidance and assistance for economies on data privacy issues, including domestic implementation of the APEC Privacy Framework, is a key role of the Data Privacy Sub-Group and can be addressed through capacity building activities.

OVERVIEW OF CBPR SYSTEM

In November 2004, Ministers for the twenty-one APEC Member Economies endorsed the APEC Privacy Framework[2]. The Framework comprises nine privacy principles and guidance on implementation to assist APEC members in developing consistent domestic approaches to personal information privacy protections. It also forms the basis for the development of a regional approach to promote accountable and responsible transfers of personal information between APEC member economies.

The APEC Data Privacy Pathfinder was endorsed by APEC Ministers in September 2007. The goal of the Data Privacy Pathfinder is to develop a simple and transparent system that can be used by organisations for the protection of personal information that moves across APEC member economies. Domestic laws or other regulatory requirements will continue to cover the collection and management of personal information within economies.

The aim of an APEC system to protect personal information that moves across borders is to encourage organizations to develop and implement their own internal business rules on privacy policies and procedures in accordance with certain requirements governing the movement of personal information across borders. These business rules developed by organizations are known as cross-border privacy rules. The purpose of the Pathfinder is to develop a Cross-Border Privacy Rules (CBPR) system. The CBPR system relies on self-assessment by organisations and on independent assessment of compliance with the requirements of the CBPR system, including meeting the minimum standards set by the APEC Privacy Principles. It will be the responsibility of specified accountability agents to make the independent assessment and certify an organization's compliance with the requirements of the CBPR system.

The elements of the CBPR system were identified in the Pathfinder and formed the basis of project groups to develop the necessary information on each element. Documents developed through this process were subsequently endorsed by ECSG and CTI as they were completed, as follows:

- a detailed self-assessment questionnaire based on the nine APEC Privacy Principles for use by an applicant organization[3];
- a set of baseline program requirements based on the nine APEC Privacy Principles against which an APEC-recognized Accountability Agent will assess an organization's completed questionnaire[4];
- recognition criteria to be used by the Joint Oversight Panel when considering the recognition of an Accountability Agent[5];
- the Cross Border Privacy Enforcement Arrangement[6] (CPEA); and
- the Charter of the Cross Border Privacy Rules Joint Oversight Panel[7] (JOP).

[2] Part IV of the Framework dealing with (a) guidance for domestic implementation and (b) guidance for international implementation was completed and endorsed by Ministers in 2005.
[3] See Project 1, CBPR Intake Questionnaire, 2011/SOM1/ECSG/DPS/020
[4] See Project 3, CBPR Program Requirements for use by Accountability Agents
[5] See Project 2, Accountability Agent Recognition Criteria, 2010/SOM1/ECSG/DPS/011
[6] See Projects 5/6/7, The Cross Border Privacy Enforcement Cooperation Arrangement, 2010/SOM1/ECSG/DPS/013

The CBPR system does not change or take the place of an Economy's domestic laws and regulations. Participating organizations continue to need to comply with relevant domestic laws and regulations for the economies in which they operate as well as the requirements of the CBPR system for personal information that moves across borders.

The CBPR system only covers the transfer of personal information to another Economy. In the simplest case personal information is collected locally in one APEC Economy and is subsequently transferred to another APEC Economy. The concept of 'transfer' includes situations where the personal information is accessed remotely from another APEC Economy.

The purpose of the CBPR system is to ensure that personal information continues to be protected, in accordance with the requirements of the CBPR program requirements, when it is transferred to any other participating APEC Member Economy. Under the CBPR system, these protections, in place at the time of collection, will be enforced by a CBPR-certified Accountability Agent, against the CBPR program requirements.

APEC economies have different approaches to protecting personal information. For example, some economies use government agencies, such as consumer protection or data protection authorities; or privacy commissioners; or other public sector regulators. Some economies also use private sector bodies, such as privacy 'trust marks,' to further consumer privacy protections. Both the regulators and the private sector bodies are concerned with ensuring that organizations are accountable for their privacy practices. In the CBPR system accountability agents can be from the public or private sectors, and might have different or overlapping roles.

At the moment, accountability agents are often limited in their ability to deal with complaints that involve activities in a different Economy. To make a system to protect personal information work effectively across borders, the system must allow accountability agents to share or transfer complaints. The aim is to ensure that the complaint is resolved by the action of one or more accountability agents in one or more economies. Consumers will also benefit from a simple complaint handling process no matter where they are located.

ROLL-OUT PLAN

Upon endorsement, the Data Privacy Subgroup will begin the process of practical implementation of the CBPR system. Key activities include, but are not limited to:

- Establishment of the JOP membership;
- Development of the CBPR system website;
- Ongoing facilitation of Economy-level participation; and
- Recognition of eligible Accountability Agents, as appropriate.

[7] See Charter of the Cross Border Privacy Rules Joint Oversight Panel, Annex A to Project 8, the APEC Cross-Border Privacy System – Policies, Rules and Guidelines

PATHFINDER PROJECTS ENDORSEMENT BACKGROUND

Singapore July/August 2009

The DPS, ECSG and CTI endorsed:

- Pathfinder projects 5, 6 and 7 establishing the APEC Cross-Border Privacy Enforcement Arrangement.

Japan, Sendai, September 2010

The DPS ECSG and CTI endorsed:

- Pathfinder project 1 – self-assessment questionnaire for organizations; and
- Pathfinder project 2 – recognition criteria for public and private sector Accountability Agents.

United States, Washington, March (by ECSG)/August 2011 (by CTI)

The DPS, ECSG and CTI endorsed:

- Pathfinder project 3 - CBPR program requirements for use by Accountability Agents.

EDITORIAL CORRECTIONS TO PATHFINDER PROJECT DOCUMENTS

Minor modifications have been made to the previously endorsed Pathfinder project documents to ensure consistency between all documents. Modifications are editorial and do not raise matters of policy. In particular, the following modifications are noted:

- Projects 1 and 3 – alignment of question 13; and
- Project 2:
  - Re-worked purpose section to reflect the process in the Project 8 document;
  - New numbering;
  - Removed all reference to Project 8 and inserted JOP or appropriate government entity;
  - In paragraph 4, inserted the phrase “that meet the CBPR program requirements developed and endorsed by APEC member economies” to anticipate the mapping that will be required to get APEC endorsement of an AA’s program requirements; and
  - Made the signature block re-certification timeline align with the Project 8 timeline.

APEC CROSS-BORDER PRIVACY RULES SYSTEM
INTAKE QUESTIONNAIRE

GENERAL

i. Name of the Organization that is seeking certification:
_____

ii. List of subsidiaries and/or affiliates governed by your privacy policy to be covered by this certification, their location, and the relationship of each to you:
_____

iii. Organization's Contact Point for Cross Border Privacy Rules ("CBPR")
Name: _____
Title: _____
Email: _____
Phone: _____

iv. For what type(s) of personal information are you applying for certification? Please check all that apply.

Customer/ Prospective Customer_____
Employee/Prospective Employee_____
Other (Please describe)_____

v. In which economies do you, your affiliates and/or subsidiaries collect or anticipate collecting personal information to be certified under this system? Please check all that apply.

☐ Australia	☐ New Zealand
☐ Brunei Darussalam	☐ Papua New Guinea
☐ Canada	☐ Peru
☐ Chile	☐ Philippines
☐ People's Republic of China	☐ Russia
☐ Hong Kong, China	☐ Singapore
☐ Indonesia	☐ Chinese Taipei
☐ Japan	☐ Thailand
☐ Republic of Korea	☐ United States
☐ Malaysia	☐ Viet Nam
☐ Mexico	

vi. To which economies do you, your affiliates and/or subsidiaries transfer or anticipate transferring personal information to be certified under this system? Please check all that apply.

☐ Australia	☐ New Zealand
☐ Brunei Darussalam	☐ Papua New Guinea
☐ Canada	☐ Peru
☐ Chile	☐ Philippines
☐ People's Republic of China	☐ Russia
☐ Hong Kong, China	☐ Singapore
☐ Indonesia	☐ Chinese Taipei
☐ Japan	☐ Thailand

☐ Republic of Korea ☐ Malaysia ☐ Mexico	☐ United States ☐ Viet Nam

NOTICE (QUESTIONS 1-4)

The questions in this section are directed towards:

(a) ensuring that individuals understand your policies regarding personal information that is collected about them, to whom it may be transferred and for what purpose it may to be used; AND

(b) ensuring that, subject to the qualifications listed in part II, individuals know when personal information is collected about them, to whom it may be transferred and for what purpose it may be used.

General

1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.

_____ Y _____ N

a) Does this privacy statement describe how your organization collects personal information?

_____ Y _____ N

b) Does this privacy statement describe the purpose(s) for which personal information is collected?

_____ Y _____ N

c) Does this privacy statement inform individuals as to whether and/for what purpose you make personal information available to third parties?

_____ Y _____ N

d) Does this privacy statement disclose the name of your company and location, including information on how to contact you about your practices and handling of personal information upon collection? Where YES describe below.

_____ _____
Y N

e) Does this privacy statement provide information regarding the use and disclosure of an individual's personal information?

_____ _____
Y N

f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?

_____ _____
Y N

2. Subject to the qualifications listed below, at the time of collection of personal information, (whether directly or through the use of third parties acting on your behalf) do you provide notice that such information is being collected?

_____ _____
Y N

3. Subject to the qualifications listed below, at the time of collection of personal information, (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which personal information is being collected?

_____ _____
Y N

4. Subject to the qualifications listed below, at the time of collection of personal information, do you notify individuals that their personal information may be shared with third parties?

_____ _____
Y N

Qualifications to the Provision of Notice

The following are situations in which the application at the time of collection of the APEC Notice Principle may not be necessary or practical.

i. **Obviousness:** Personal Information controllers do not need to provide notice of the collection, use or third-party sharing of personal information in those circumstances where consent by the individual can be inferred from the provision of the individual's information (e.g. if an individual gives his or her business card to another individual in the context of a business relationship, the individual would not expect that notice would be provided regarding the collection and normal use of that information).

ii. Collection of Publicly-Available Information: Personal information controllers do not need to provide notice regarding the collection and use of publicly available information.

iii. Technological Impracticability: Personal Information controllers do not need to provide notice at or before the time of collection in those cases where electronic technology automatically collects information when a prospective customer initiates contact (e.g. through the use of cookies). However, the notice should be provided to the individuals as soon after as is practicable.

iv. Disclosure to a government institution which has made a request for the information with lawful authority: Personal information controllers do not need to provide notice of disclosure to law enforcement agencies for investigation purposes where the provision of such notice to the individual will likely prejudice the investigation.

v. Disclosure to a third party pursuant to a lawful form of process: Personal information controllers do not need to provide notice of disclosure to a third party when such disclosure was requested pursuant to a lawful form of process such as a discovery request made in the course of civil litigation.

vi. Third-Party Receipt: Where personal information is received from a third party, the recipient personal information controller does not need to provide notice to the individuals at or before the time of collection of the information.

vii. For legitimate investigation purposes: When providing notice would compromise the availability or accuracy of the information and the collection, use and disclosure are reasonable for purposes relating to an internal or external investigation of a violation of a code of conduct, breach of contract or a contravention of domestic law.

viii. Action in the event of an emergency: Personal Information controllers do not need to provide notice in emergency situations that threaten the life, health or security of an individual.

COLLECTION LIMITATION (QUESTIONS 5-7)

The questions in this section are directed towards ensuring that collection of information is limited to the stated 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. In all instances, collection methods must be lawful and fair.

5. How do you obtain personal information:

    a) Directly from the individual?

    _____ Y _____ N

    b) From third parties collecting on your behalf?

    _____ Y _____ N

    c) Other. If YES, describe.

    _____ Y _____ N

6. Do you limit your personal information collection (whether directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes?

    _____ Y _____ N

7. Do you collect personal information (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information? Where YES, describe.

    _____ Y _____ N

USES OF PERSONAL INFORMATION (QUESTIONS 8-13)

The questions in this section are directed toward ensuring that the use of personal information is limited to fulfilling the purposes of collection and other compatible or related purposes. This section covers use, transfer and disclosure of personal information. Application of this Principle requires consideration of the nature of the information, the context of collection and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" could extend, for example, to matters such as the creation and use of a centralized database to manage personnel in an effective and efficient manner; the processing of employee payrolls by a third party; or, the use of information collected by an organization for the purpose of granting credit for the subsequent purpose of collecting debt owed to that organization.

8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below.

_____ Y _____ N

9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below.

    a) Based on express consent of the individual?

    b) Compelled by applicable laws?

10. Do you disclose personal information you collect (whether directly or through the use of third parties acting on your behalf) to other personal information controllers? If YES, describe.

_____ Y _____ N

11. Do you transfer personal information to personal information processors? If YES, describe.

_____ Y _____ N

12. If you answered YES to question 10 and/or question 11, is the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible or related purpose? Describe below.

_____ Y _____ N

13. If you answered NO to question 12, or if otherwise appropriate, does the disclosure and/or transfer take place under one of the following circumstances?

    a) Based on express consent of the individual?

    b) Necessary to provide a service or product requested by the individual?

    c) Compelled by applicable laws?

CHOICE (QUESTIONS 14-20)

The questions in this section are directed towards ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information. However, this Principle recognizes, through the introductory words "where appropriate" in the Framework itself, that there are certain situations where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice. These situations are detailed in "Qualifications to the Provision of Choice Mechanisms".

General

14. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES describe such mechanisms below.

_____ _____
Y N

15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information? Where YES describe such mechanisms below.

_____ _____
Y N

16. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information? Where YES describe such mechanisms below.

_____ _____
Y N

17. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner?

_____ _____
Y N

18. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?

_____ _____
Y N

19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are these choices easily accessible and affordable? Where YES, describe.

_____ Y _____ N

20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.

Qualifications to the Provision of Choice Mechanisms

The following are situations in which the application of the APEC Choice Principle may not be necessary or practical.

i. **Obviousness:** Personal Information controllers do not need to provide a mechanism for individuals to exercise choice in the collection, use or third-party sharing of personal information in those circumstances where consent by the individual can be inferred from the provision of the individual's information.

ii. **Collection of Publicly-Available Information**: Personal information controllers do not need to provide a mechanism for individuals to exercise choice in relation to the collection and use of publicly available information.

iii. **Technological Impracticability**: Personal Information controllers do not need to provide a mechanism for individuals to exercise choice in relation to those cases where electronic technology automatically collects information when a prospective customer initiates contact [e.g. use of cookies]. However, a mechanism to exercise choice as to use and disclosure should be provided after collection of the information.

iv. **Third-Party Receipt**: Where personal information is received from a third party, the recipient personal information controller does not need to provide a mechanism for individuals to exercise choice in relation to the collection of the information. However, if the personal information controller engages a third party to collect personal information on its behalf, the personal information controller should instruct the collector to provide such choice when collecting the personal information.

v. **Disclosure to a government institution which has made a request for the information with lawful authority**: Personal Information controllers do not need to provide a mechanism for individuals to exercise choice in relation to disclosure to law enforcement agencies for investigation purposes where the provision of such mechanism to the individual will likely prejudice the investigation.

vi. **Disclosure to a third party pursuant to a lawful form of process:** Personal information controllers do not need to provide a mechanism for individuals to exercise choice in relation to the disclosure to a third party when such disclosure was requested pursuant to a lawful form of process such as a discovery request made in the course of civil litigation.

vii. **For legitimate investigation purposes**: When providing a mechanism for individuals to exercise choice would compromise the availability or accuracy of the personal information and its collection, use and disclosure are reasonable for purposes relating to an internal or external investigation of a violation of a code of conduct, breach of contract or a contravention of domestic law.

viii. **Action in the event of an emergency**: Personal Information controllers do not need to provide a mechanism for individuals to exercise choice in emergency situations that threaten the life, health or security of an individual.

INTEGRITY OF PERSONAL INFORMATION (QUESTIONS 21-25)

The questions in this section are directed towards ensuring that the personal information controller maintains the accuracy and completeness of records and keeps them up to date. This Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use.

21. Do you take steps to verify that the personal information held by you is up to date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe.

_____ Y _____ N

22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use? Provide a description in the space below or in an attachment if necessary.

_____ Y _____ N

23. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the transfer of the information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal information was transferred? If YES, describe.

_____ Y _____ N

24. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the corrections to other third parties to whom the personal information was disclosed? If YES, describe.

25. Do you require personal information processors, agents, or other service providers who act on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?

_____ Y _____ N

SECURITY SAFEGUARDS (QUESTIONS 26-35)

The questions in this section are directed towards ensuring that when individuals entrust their information to an organization, their information will be protected with reasonable security safeguards to prevent loss or unauthorized access to personal information or unauthorized destruction, use, modification or disclosure of information or other misuses.

26. Have you implemented an information security policy?

_____ Y _____ N

27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?

28. Describe how the safeguards you identified in response to question 27 are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.

29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).

30. Have you implemented safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held through:

    a) Employee training and management or other organizational safeguards?

    _____ Y _____ N

    b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal?

    _____ Y _____ N

    c) Detecting, preventing, and responding to attacks, intrusions, or other security failures?

    _____ Y _____ N

    d) Physical security?

    _____ Y _____ N

31. Have you implemented a policy for secure disposal of personal information?

_____ Y _____ N

32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?

_____ Y _____ N

33. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 32? Describe below.

_____ Y _____ N

34. Do you use third-party certifications or other risk assessments? Describe below.

_____ Y _____ N

35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by:

    a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided?

    _____ Y _____ N

    b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of your organization's personal information?

    _____ Y _____ N

    c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?

    _____ Y _____ N

ACCESS AND CORRECTION (QUESTIONS 36-38)

The questions in this section are directed towards ensuring that individuals are able to access and correct their information. This section includes specific conditions for what would be considered reasonable in the provision of access. Access will also be conditioned by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access. The details of the procedures by which the ability to access and correct information is provided may differ depending on the nature of the information and other interests. For this reason, in certain circumstances, it may be impossible, impracticable or unnecessary to change, suppress or delete records.

The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right. While you should always make good faith efforts to provide access, in some situations, it may be necessary to deny claims for access and correction. "Qualifications to the Provision of Access and Correction" sets out those conditions that must be met in order for such denials to be considered acceptable. When you deny a request for access, for the reasons specified herein, you should provide the requesting individual with an explanation as to why you have made that determination and information on how to challenge that denial. You would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order.

General

36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.

_____ _____
Y N

37. Upon request, do you provide individuals access to the personal information that you hold about them? Where YES, answer questions 37(a) – (e) and describe your organization's policies/procedures for receiving and handling access requests below. Where NO, proceed to question 38

_____ _____
Y N

a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe.

_____ _____
Y N

b) Do you provide access within a reasonable timeframe following an individual's request for access? If YES, please describe.

_____ _____
Y N

c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe.

_____ _____
Y N

d) Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc)?

_____ _____
Y N

e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.

_____ _____
Y N

38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your organization's policies/procedures in this regard below and answer questions 38 (a), (b), (c), (d) and (e).

_____ _____
Y N

a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary.

_____ _____
Y N

b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion?

_____ _____
Y N

c) Do you make such corrections or deletions within a reasonable timeframe following an individual's request for correction or deletion?

_____ _____
Y N

d) Do you provide a copy of the corrected personal information or provide confirmation that the data has been corrected or deleted to the individual?

_____ _____
Y N

e) If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?

_____ _____
Y N

Qualifications to the Provision of Access and Correction Mechanisms

Although organizations should always make good faith efforts to provide access, there are some situations, described below, in which it may be necessary for organizations to deny access requests. Please identify which, if any, of these situations apply, and specify their application to you, with reference to your responses provided to the previous questions, in the space provided.

i. **Disproportionate Burden:** Personal information controllers do not need to provide access and correction where the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question, as for example when claims for access are repetitious or vexatious by nature.

ii. **Protection of Confidential Information:** Personal information controllers do not need to provide access and correction where the information cannot be disclosed due to legal or security reasons or to protect confidential commercial information (i.e. information that you have taken steps to protect from disclosure, where such disclosure would facilitate a competitor in the market to use or exploit the information against your business interest causing significant financial loss). Where confidential commercial information can be readily separated from other information subject to an access request, the personal information controller should redact the confidential commercial information and make available the non-confidential commercial information to the extent that such information constitutes personal information of the individual concerned. Other situations would include those where disclosure of information would benefit a competitor in the market place, such as a particular computer or modeling program. Furthermore, a denial of access may also be considered acceptable in situations where, for example providing the information would constitute a violation of laws or would compromise security.

iii. **Third Party Risk:** Personal information controllers do not need to provide access and correction where the information privacy of persons other than the individual would be violated. In those instances where a third party's personal information can be severed from the information requested for access or correction, the personal information controller must release the information after redaction of the third party's personal information.

ACCOUNTABILITY (QUESTIONS 39-51)

The questions in this section are directed towards ensuring that you are accountable for complying with measures that give effect to the Principles stated above. Additionally, when transferring information, you should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.

General

39. What measures does your organization take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe below.

    - Internal guidelines or policies (if applicable, describe how implemented) _____
    - Contracts _____
    - Compliance with applicable industry or sector laws and regulations ____
    - Compliance with self-regulatory organization code and/or rules ____
    - Other (describe) ____

40. Has your organization appointed an individual(s) to be responsible for your organization's overall compliance with the Privacy Principles?

    _____ Y _____ N

41. Does your organization have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.

    _____ Y _____ N

42. Does your organization have procedures in place to ensure individuals receive a timely response to their complaints?

    _____ Y _____ N

43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.

    _____ Y _____ N

44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.

_____ _____
Y N

45. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information?

_____ _____
Y N

Maintaining Accountability When Personal Information is Transferred

46. Do you have mechanisms in place with personal information processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)?
    - *Internal guidelines or policies* _____
    - *Contracts* _____
    - *Compliance with applicable industry or sector laws and regulations* _____
    - *Compliance with self-regulatory organization code and/or rules* _____
    - *Other (describe)* _____

47. Do these mechanisms generally require that personal information processors, agents, contractors or other service providers:

    - Abide by your APEC-compliant privacy policies and practices as stated in your Privacy Statement? _____

    - Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement? _____

    - Follow instructions provided by you relating to the manner in which your personal information must be handled? _____

    - Impose restrictions on subcontracting unless with your consent? _____

    - Have their CBPRs certified by an APEC accountability agent in their jurisdiction? _____

    - Other (describe) _____

48. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.

_____ _____
Y N

49. Do you carry out regular spot checking or monitoring of your personal information processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.

_____ _____
Y N

50. Do you disclose personal information to other personal information controllers in situations where due diligence and mechanisms to ensure compliance with your APEC CBPRs by the recipient as described above is impractical or impossible?

_____ _____
Y N

ACCOUNTABILITY AGENT RECOGNITION CRITERIA

The purpose of this document is to set out the criteria necessary for an Accountability Agent to participate in the APEC Cross-Border Privacy Rules System. The applicant must submit this form and appropriate supporting documentation to the relevant government agency or public authority for initial review. The agency or authority will forward all information received to the Joint Oversight Panel to consider recommending the applicant for recognition by member economies as an APEC Cross-Border Privacy Rules System Accountability Agent.

CRITERIA

Conflicts of Interest

1) General Requirements

   a. An Accountability Agent must be free of actual or potential conflicts of interest in order to participate in the APEC Cross Border Privacy Rules (CBPR) System. For the purposes of participation as an Accountability Agent in the CBPR System, this means the ability of the Accountability Agent to perform all tasks related to an Applicant's certification and ongoing participation in the CBPR System free from influences that would compromise the Accountability Agent's professional judgment, objectivity and integrity.

   b. An Accountability Agent must satisfy the APEC member economies with evidence that internal structural and procedural safeguards are in place to address potential and actual conflicts of interest. Such safeguards should include but not be limited to:

      i. Written policies for disclosure of potential conflicts of interest and, where appropriate, withdrawal of the Accountability Agent from particular engagements. Such withdrawal will be required in cases where the Accountability Agent is related to the Applicant or Participant to the extent that it would give rise to a risk that the Accountability Agent's professional judgment, integrity, or objectivity could be influenced by the relationship.

      ii. Written policies governing the separation of personnel handling privacy certification functions from personnel handling sales and consulting functions.

      iii. Written policies for internal review of potential conflicts of interest with Applicants and Participants.

      iv. Published certification standards for Applicants and Participants (see paragraph 4 'Program Requirements').

      v. Mechanisms for regular reporting to the relevant government agency or public authority on certification of new Applicants, audits of existing Participants, and dispute resolution.

      vi. Mechanisms for mandatory publication of case reports in certain circumstances.

2) Requirements with respect to particular Applicants and/or Participants

a. At no time may an Accountability Agent have a direct or indirect affiliation with any Applicant or Participant that would prejudice the ability of the Accountability agent to render a fair decision with respect to their certification and ongoing participation in the CBPR System, including but not limited to during the application review and initial certification process; during ongoing monitoring and compliance review; during re-certification and annual attestation; and during dispute resolution and enforcement of the Program Requirements against a Participant. Such affiliations, which include but are not limited to the Applicant or Participant and the Accountability Agent being under common control such that the Applicant or Participant can exert undue influence in the Accountability Agent, constitute relationships that require withdrawal under 1(b)(i).

b. For other types of affiliations that may be cured by the existence of structural safeguards or other procedures undertaken by the Accountability Agent, the existence of any such affiliations between the Accountability Agent and the Applicant or Participant must be disclosed promptly to the Joint Oversight Panel, together with an explanation of the safeguards in place to ensure that such affiliations do not compromise the Accountability Agent's ability to render a fair decision with respect to such an Applicant or Participant. Such affiliations include but are not limited to:

    i. officers of the Applicant or Participant serving on the Accountability Agent's board of directors in a voting capacity, and vice versa;

    ii. significant monetary arrangements or commercial relationship between the Accountability Agent and the Applicant or Participant, outside of the fee charged for certification and participation in the APEC CBPR System; or

    iii. all other affiliations which might allow the Applicant or Participant to exert undue influence on the Accountability Agent regarding the Applicant's certification and participation in the CBPR System.

c. Outside of the functions described in paragraphs 5-14 of this document, an Accountability Agent will refrain from performing for its Participants or Applicants services for a fee or any interest or benefit such as the following categories:

    i. consulting or technical services related to the development or implementation of Participant's or Applicant's data privacy practices and procedures;

    ii. consulting or technical services related to the development of its privacy policy or statement; or

    iii. consulting or technical services related to its security safeguards.

d. An Accountability Agent may be engaged to perform consulting or technical services for an Applicant or Participant other than services relating to their certification and

on-going participation in the CBPR System. Where this occurs, the Accountability Agent will disclose to the Joint Oversight Panel:

i. the existence of the engagement; and

ii. an explanation of the safeguards in place to ensure that the Accountability Agent remains free of actual or potential conflicts of interest arising from the engagement [*such safeguards may include segregating the personnel providing the consulting or technical services from the personnel performing the functions described in paragraphs 5 -14 of this document*].

e. Provision of services as required in Sections 3 through 6 shall not be considered performing consulting services which might trigger a prohibition contained in this document.

3) In addition to disclosing to the Joint Oversight Panel all withdrawals described above in Section 1(b)(i), an Accountability Agent also shall disclose to the Joint Oversight Panel those activities or business ventures identified in subsection 1(b) above that might on their face have been considered a conflict of interest but did not result in withdrawal. Such disclosures should include a description of the reasons for non-withdrawal and the measures the Accountability Agent took to avoid or cure any potential prejudicial results stemming from the actual or potential conflict of interest.

Program Requirements

4) An Accountability Agent evaluates Applicants against a set of program requirements that encompass all of the principles of the APEC Privacy Framework with respect to cross border data transfers and that meet the CBPR program requirements developed and endorsed by APEC member economies (to be submitted along with this form). (*NOTE:* an Accountability Agent may charge a fee to a Participant for provision of these services without triggering the prohibitions contained in paragraph 1 or 2.)

Certification Process

5) An Accountability Agent has a comprehensive process to review an Applicant's policies and practices with respect to the Applicant's participation in the Cross Border Privacy Rules System and to verify its compliance with the Accountability Agent's program requirements. The certification process includes:

a) An initial assessment of compliance, which will include verifying the contents of the self-assessment forms completed by the Applicant against the program requirements for Accountability Agents, and which may also include in-person or phone interviews, inspection of the personal data system, Web site scans, or automated security tools.

b) A comprehensive report to the Applicant outlining the Accountability Agent's findings regarding the Applicant's level of compliance with the program requirements. Where non-fulfillment of any of the program requirements is found, the report must include a list of changes the Applicant needs to complete for purposes of obtaining certification for participation in the CBPR System.

c) Verification that any changes required under subsection (b) have been properly completed by the Applicant.

d) Certification that the Applicant is in compliance with the Accountability Agent's program requirements. An Applicant that has received such a certification will be referred to herein as a "Participant" in the CBPR System.

On-going Monitoring and Compliance Review Processes

6) Accountability Agent has comprehensive written procedures designed to ensure the integrity of the Certification process and to monitor the Participant throughout the certification period to ensure compliance with the Accountability Agent's program.

7) In addition, where there are reasonable grounds for the Accountability Agent to believe that a Participant has engaged in a practice that may constitute a breach of the program requirements, an immediate review process will be triggered whereby verification of compliance will be carried out. Where non-compliance with any of the program requirements is found, the Accountability Agent will notify the Participant outlining the corrections the Participant needs to make and a reasonable timeframe within which the corrections must be completed. The Accountability Agent must verify that the required changes have been properly completed by the Participant within the stated timeframe.

Re-Certification and Annual Attestation

8) Accountability Agent will require Participants to attest on an annual basis to the continuing adherence to the CBPR program requirements. Regular comprehensive reviews will be carried out to ensure the integrity of the re-Certification. Where there has been a material change to the Participant's privacy policy (as reasonably determined by the Accountability Agent in good faith), an immediate review process will be carried out. This re-certification review process includes:

a) An assessment of compliance, which will include verification of the contents of the self-assessment forms (Project 1) updated by the Participant, and which may also include in-person or phone interviews, inspection of the personal data system, Web site scans, or automated security tools.

b) A report to the Participant outlining the Accountability Agent's findings regarding the Participant's level of compliance with the program requirements. The report must also list any corrections the Participant needs to make to correct areas of non-compliance and the timeframe within which the corrections must be completed for purposes of obtaining re-certification.

c) Verification that required changes have been properly completed by Participant.

d) Notice to the Participant that the Participant is in compliance with the Accountability Agent's program requirements and has been re-certified.

Dispute Resolution Process

9) An Accountability Agent must have a mechanism to receive and investigate complaints about Participants and to resolve disputes between complainants and Participants in

relation to non-compliance with its program requirements, as well as a mechanism for cooperation on dispute resolution with other Accountability Agents recognized by APEC economies when appropriate and where possible. An Accountability Agent may choose not to directly supply the dispute resolution mechanism. The dispute resolution mechanism may be contracted out by an Accountability Agent to a third party for supply of the dispute resolution service. Where the dispute resolution mechanism is contracted out by an Accountability Agent the relationship must be in place at the time the Accountability Agent is certified under the APEC CBPR system.

10) The dispute resolution process, whether supplied directly or by a third party under contract, includes the following elements:

    a) A process for receiving complaints and determining whether a complaint concerns the Participant's obligations under the program and that the filed complaint falls within the scope of the program's requirements.

    b) A process for notifying the complainant of the determination made under subpart (a), above.

    c) A process for investigating complaints.

    d) A confidential and timely process for resolving complaints. Where non-compliance with any of the program requirements is found, the Accountability Agent or contracted third party supplier of the dispute resolution service will notify the Participant outlining the corrections the Participant needs to make and the reasonable timeframe within which the corrections must be completed.

    e) Written notice of complaint resolution by the Accountability Agent or contracted third party supplier of the dispute resolution service to the complainant and the Participant.

    f) A process for obtaining an individual's consent before sharing that individual's personal information with the relevant enforcement authority in connection with a request for assistance.

    g) A process for making publicly available statistics on the types of complaints received by the Accountability Agent or contracted third party supplier of the dispute resolution service and the outcomes of such complaints, and for communicating that information to the relevant government agency and privacy enforcement authority.

    h) A process for releasing in anonymised form, case notes on a selection of resolved complaints illustrating typical or significant interpretations and notable outcomes (see Annex A).]

Mechanism for Enforcing Program Requirements

11) Accountability Agent has the authority to enforce its program requirements against Participants, either through contract or by law.

12) Accountability Agent has a process in place for notifying Participant immediately of non-compliance with Accountability Agent's program requirements and for requiring Participant to remedy the non-compliance within a specified time period.

13) Accountability Agent has processes in place to impose the following penalties, which is proportional to the harm or potential harm resulting from the violation, in cases where a Participant has not complied with the program requirements and has failed to remedy the non-compliance within a specified time period. [*NOTE*: In addition to the penalties listed below, Accountability Agent may execute contracts related to legal rights and, where applicable, those related intellectual property rights enforceable in a court of law.]

    a) Requiring Participant to remedy the non-compliance within a specified time period, failing which the Accountability Agent shall remove the Participant from its program.

    b) Temporarily suspending the Participant's right to display the Accountability Agent's seal.

    c) Naming the Participant and publicizing the non-compliance.

    d) Referring the violation to the relevant public authority or privacy enforcement authority. [*NOTE*: this should be reserved for circumstances where a violation raises to the level of a violation of applicable law.]

    e) Other penalties – including monetary penalties – as deemed appropriate by the Accountability Agent.

14) Accountability Agent will refer a matter to the appropriate public authority or enforcement agency for review and possible law enforcement action, where the Accountability Agent has a reasonable belief pursuant to its established review process that a Participant's failure to comply with the APEC Cross-Border Privacy Rules System requirements has not been remedied within a reasonable time under the procedures established by the Accountability Agent pursuant to paragraph 2 so long as such failure to comply can be reasonably believed to be a violation of applicable law.

15) Where possible, Accountability Agent will respond to requests from enforcement entities in APEC Economies that reasonably relate to that Economy and to the CBPR-related activities of the Accountability Agent.

SIGNATURE AND CONTACT INFORMATION

By signing this document, the signing party attests to the truth of the answers given.

_____ _____

[Signature of person who has authority to commit party to the agreement] **[Date]**

[Typed name]

[Typed title]

[Typed name of organization]

[Address of organization]

[Email address]

[Telephone number]

APEC recognition is limited to one year from the date of recognition. Each year one month prior to the anniversary of the date of recognition, the Accountability Agent must resubmit this form and any associated documentation to the appropriate government agency or public authority or as soon as practicable in the event of a material change (e.g. ownership, structure, policies).

NOTE: Failure to comply with any of the requirements outlined in this document may result in appropriate sanctions under applicable domestic law.

Annex A

ACCOUNTABILITY AGENT CASE NOTE TEMPLATE

The Accountability Agent Recognition Criteria require applicants to attest that as part of their dispute resolution mechanism they have a process for releasing, in anonymised form, case notes on a selection of resolved complaints illustrating typical or significant interpretations and notable outcomes.

The template, with associated guidance and FAQs, will assist in meeting the requirement.

Objectives of Release of Case Notes

Complaints handling is an important element of the Cross-border Privacy Rules (CBPR) program. The recognition criteria for Accountability Agents include an obligation to release case notes on a selection of resolved complaints in order to:

- promote understanding about the operation of the CBPR program;
- assist consumers and businesses and their advisers;
- facilitate consistency in the interpretation of the APEC information privacy principles and the common elements of the CBPR program;
- increase transparency in the CBPR program; and
- promote accountability of those involved in complaints handling and build stakeholder trust in accountability agents.

Commentary on the Template

The template is provided as a tool for Accountability Agents. It is acceptable to depart from the template for stylistic reasons by, for example, reordering the elements (e.g. by switching the date and citation to different ends of the note) or adding additional elements. However, it would be difficult to produce a satisfactory case note without the minimum elements mentioned in the template.

General heading
It is possible to combine the general heading and citation into a single heading or adopt a citation that stands in for a general heading. However, unlike a series of law reports directed exclusively at lawyers, case notes are useful as an educational tool for ordinary consumers and businesses. Accordingly, a general heading that communicates a clear straightforward message is recommended.

Citation
It is essential that all those that may wish to refer to a case note can do so by an accepted citation that unambiguously refers to the same note. All case notes should be issued with a citation including the following elements:

- a descriptor of the case;
- the year of publication ;
- a standard abbreviation for the accountability authority (including an indicator of which economy the Accountability Agent is based), and;
- a sequential number.

Case report

The style and approach of case reports can differ substantially but there are several elements that almost certainly will appear. These include:

- an account of the facts (e.g. as initially asserted on a complaint and as found after investigation)
- the relevant law (which will include the elements of the CBPR program)
- a discussion of the issues of interest and how the law applied to the facts in question
- the outcome of the complaint.

Key terms

It may be useful to include the standard terms used in traditional indexing or which will appear as tags in on-line environments.

CASE NOTE TEMPLATE

General heading
Citation
Case report · Facts · Law · Discussion · Outcome
Date
Key terms · Tags

FREQUENTLY ASKED QUESTIONS

Q. *How many case notes should an Accountability Agent publish?*

A. Those responsible for a CBPR program may find it useful to set targets for how many case notes should be published and make those targets public. In the initial years of a scheme's operation a greater number of case notes may be warranted so as to assist advisers and to provide reassurance to regulators and others. In later years, when there is a greater body of case notes available, fewer new notes may be needed. A scheme handling very few complaints will need to report a greater proportion of its complaints than a large scheme which can be more selective. As a general guide, a scheme handling more than 200 complaints a year might aim to publish about 8-10% of that number in case notes in the early years dropping later to, perhaps, 3–5 %.

Q. Which resolved complaints should be selected for case notes?

A. Those responsible for a CBPR program may find it useful to adopt standards to be applied in selecting case suitable for reporting. For instance, to ensure that the more serious cases are identified for reporting, criteria might refer to such indicators of systemic impact such as size of monetary settlements or awards. There is a need to report cases including significant or novel interpretations. There is also a value in reporting some typical cases which raise no novel legal issues but which illustrate the operation of the CBPR program in action.

Q. *Why are case notes typically reported in anonymous form?*

A. Case notes seek to illustrate the operation of the CBPR scheme, to educate about matters of interpretation and to ensure those handling complaints remain accountable. These objectives do not necessarily require the respondent to be named. The major objective of the complaints system is to resolve consumer disputes. Subject to the requirements of any particular scheme, this is often facilitated by confidential conciliation or mediation between the parties which does not require, and may even be hampered by, naming respondents publicly.

Q. *Might it be useful to name respondents sometimes?*

A. Sometimes it will be appropriate to name the respondent to a complaint. Indeed, some CBPR programs might have this as their usual practice. Even programs that do not usually name respondents may need to do so sometimes, for instance where the respondent has publicly announced that the program is handling the complaint or that fact has otherwise become a matter of public notoriety. Occasionally, naming a respondent is an intentional part of the complaint outcome (e.g. if the respondent is refusing to cooperate with the investigation or accept the outcome). It will be good practice for Accountability Agents to adopt transparent policies on their practices for naming respondents.

Q. *How much detail should appear in the case notes?*

A. When publishing case notes in anonymous form, care needs to be taken in publishing details which might inadvertently identify the parties. Anonymity is usually easily achieved through generalizing factual details. The level of useful detail in a particular case note will depend upon why it has been chosen for reporting. For example, complaints selected for a case

note to illustrate a novel matter of legal interpretation will need the legal reasoning to be set out in full detail. By contrast, a case note illustrating a fairly routine interpretation in an interesting factual setting will obvious pay more attention to the facts. In the early phases of a scheme, relatively simple case notes are acceptable to ensure that advisers understand basic concepts but these should be followed by more detailed notes as familiarity with basic concepts is established.

Q *How should Accountability Agents disseminate case notes?*

A. Active steps should be taken to make case notes easily available. Useful approaches may include to:

- maintain a distribution list to which copies of case notes are emailed
- release case notes individually or in batches during the year with accompanying media statements
- prepare summaries and use these in newsletters to highlight the release of new case notes
- post case notes on the Accountability Agent's website with good indexing and retrieval tools
- distribute electronic copies through RSS feeds
- integrate case notes into other educative initiatives such as training packages
- co-operate in re-publication by legal publishers.

Q. *How can Accountability Agents assist in making case notes readily available throughout the Asia Pacific?*

A. The cross-border nature of a CBPR program means that case notes will be useful to consumers, businesses, regulators and advisers in a variety of economies and not just in the Accountability Agent's home economy. Extra efforts should be taken to make their case notes widely available. These extra efforts will also contribute to consistency in interpretation across the region. Two key steps that Accountability Agents can take to make their case notes accessible throughout the Asia Pacific include:

- to facilitate the efforts of those who wish to re-publish their case notes
- to provide their case notes, in electronic form, to a recognised international consolidated point of access.

Q. How can Accountability Agents facilitate the efforts of those who wish to republish their case notes?

A. Third party publishers can enable case notes to be made more widely available to the public, specialist bodies, advisers, researchers and regulators. Accountability Agents may facilitate re-publication by giving a general license for re-publication of case notes with proper acknowledgement. The general license should be included with the usual copyright statement posted on an Accountability Agent's website.

Q. Is there a place where all case notes could be deposited and accessed?

A. There is considerable value in having consolidated point of access for case notes from a variety of privacy enforcement authorities and accountability agents. The World Legal Information Institute's International Privacy Law Library available at

www.worldlii.org/int/special/privacy provides a specialist facility for hosting privacy case notes and has for many years published case notes from privacy enforcement authorities in various Asia Pacific economies. The consolidated access point brings a variety of benefits including the ability to search seamlessly across a range of case note series from within the region. Accountability Agents are encouraged to make arrangements with WorldLII for the supply of case notes and their republication.

Q. *Is there any further published guidance on releasing case notes?*

A. The following resources discuss issues in releasing case notes and provide examples:

- International Privacy Law Library available at www.worldlii.org/int/special/privacy - which includes many examples of privacy case note series
- Graham Greenleaf, 'Reforming Reporting of Privacy Cases: A Proposal for Improving Accountability for Asia-Pacific Privacy Commissioners', 2004 available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=512782
- Asia-Pacific Privacy Authorities Statement of Common Administrative Practice on Case Note Citation, November 2005, available at www.privacy.gov.au/international/appa/statement.pdf
- Asia-Pacific Privacy Authorities Statement of Common Administrative Practice on Case Note Dissemination, November 2006, available at www.privacy.gov.au/international/appa/statement2.pdf
- OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy, 2007, clause 20, available at www.oecd.org/dataoecd/43/28/38770483.pdf

Annex B

ACCOUNTABILITY AGENT COMPLAINT STATISTICS

The Accountability Agent recognition criteria require applicants to attest that as part of their dispute resolution mechanism they have a process for releasing complaint statistics and for communicating that information to the relevant government agency and privacy enforcement authority.

The template, with associated guidance and FAQs will assist in meeting the requirement.

Objectives of Reporting Complaint Statistics

Complaints handling is an important element of the Cross-Border Privacy Rules (CBPR) program. The recognition criteria for Accountability Agents include an obligation to publish and report statistics on complaints received in order to:

- promote understanding about the operation of the CBPR program;
- increase transparency across the CBPR system;
- help governments, business and others to see how a complaints system is working and to help identify trends;
- enable comparisons of parts of the CBPR program across the APEC region; and
- promote accountability of those involved in complaints handling and build stakeholder trust in Accountability Agents.

Commentary on the Template

The template is provided as a tool for accountability agents. It is acceptable to depart from the template by reporting additional statistics. However, the core minimum statistics should be reported in each case since they will form a common and comparable minimum data set across all APEC Accountability Agent dispute resolution processes. In particular jurisdictions, governmental authorities may require the reporting of additional statistics.

Complaint numbers
The total number of complaints should be reported. A format for reporting will need to be adopted that makes clear the number of new complaints received as well as older complaints carried over from the previous reporting period.

To assist readers to understand the reported figures and to aid in comparability there should be a note as to how terms are being used. For instance, some matters may be on the borderline between an enquiry about a company's information practice of concern and a complaint about that practice. Such matters may be quickly sorted out with an explanation to the enquirer or perhaps a telephone call to the company. Some programs may treat all matters as complaints while others may reserve that term for more formal dispute resolution or investigation and have another category for the matters treated less formally.

Complaint outcomes
This part of the template provides a picture of the processing of complaints.

Complaints type
The template asks Accountability Agents to provide informative breakdowns of the complaints by type. This will provide a statistical picture of who is complaining and why.

Some complaints will raise several different issues. The report should explain the basis upon which the Accountability Agent is reporting. One approach is, for example, to identify the principal aspect of the complaint and treat it for statistical purposes as being only about that issue. An alternative is to count and classify all the allegations made in a complaint. If the latter approach is taken, the totals of complaint types will exceed the total number of complaints received and this will need to be explained or it may seem to be an anomaly.

Complaints process quality measures

There statistics give a picture as to how well the complaints resolution system is working. At a minimum, some indication as to timeliness should be reported. At its simplest this might be to highlight the number or complaints that took longer than a target date to resolve (e.g. number of complaints on hand that are older than, say, three months) while some complaints systems may be able to produce a variety of more detailed statistics (e.g. the average time to resolve certain types of complaints). In a more sophisticated system other quality measures may be included and an Accountability Agent might, for example, report against internal targets or industry benchmarks if these are available.

General

The Accountability Agent should comment on the various figures reported. To set the statistics in context, it is useful to include three or four years of figures where these are available.

COMPLAINT STATISTICS TEMPLATE

Complaint Numbers

Number of complaints received during the year with a comment by the Accountability Agent on the significance of the number. A note should explain how the term 'complaint' is being used in the reported statistics.

Complaint Processing and Outcomes

Complaints processed during the year broken down by the outcome.

Examples of typical outcomes include:

- complaints that could not be handled as they were outside the program's jurisdiction (e.g. against a company that is not part of the CBPR program);
- complaints referred back to a business that are resolved at that point;
- complaints settled by the Accountability Agent;
- complaints transferred to another Accountability Agent, Privacy Enforcement Authority or other enforcement authority;
- complaints for which the Accountability Agent has made a finding (such as complaint dismissed, complaint upheld in part, complaint upheld in full).

When the Accountability Agent has made findings upholding complaints, further statistical information should be given about the outcomes and any subsequent enforcement action.

The Accountability Agent should include a comment on the significance of the complaints outcomes.

Complaints Type

Further statistics should be provided as to the type of complaints, including the subject matter of the complaint and characterization of the complainants and the respondents. Useful classifications will include:

- complaint subject matter broken down by APEC information privacy principle (notice, collection limitation, use, etc);
- basic information about complainants, where known, such as the economy from which complaints have been made;
- Information about the type of respondents to complaints – this will vary on the nature of a particularly CBPR program but may include industry classification (e.g. financial service activities, insurance), the capacity in which the respondent falls (e.g. information processor, employer, service provider), or size of company (SME, large company etc).

The Accountability Agent should comment on the significance of the reported figures.

Complaints Process Quality Measures

An indication should be given as to about any quality measures used in relation to the particular CBPR program. A typical measure may relate to timeliness. The Accountability Agent should offer a comment upon the figures reported.

FREQUENTLY ASKED QUESTIONS

Q. *Why does APEC require complaint statistics to be released?*

A. Complaints statistics are part of a transparent and accountable complaints handling system. The statistics will help paint a picture of how the CBPR program is operating. A number of stakeholders have an interest in seeing such a picture. For example, companies within a CBPR program, consumer advocates and regulators all have interest in knowing what happens in relation to the processing of complaints through an Accountability Agent. Transparency will promote understanding and confidence in the system.

Q. *Why do I need to release statistics on all the topics in the template?*

A. The template lists a minimum set of statistics that should be reported. To get a complete picture, all the categories of statistics are needed. Furthermore, since these are standard requirements across all APEC economies, the resultant statistics should be reasonably comparable. Over time, a picture should emerge as to how well CBPR programs are working and whether change is desirable.

Q. *How should these statistics be presented?*

A. The template provides the statistics that should be reported and requires that the Accountability Agent comment upon the significance of the figures. It is recommended that the statistics reported for a particular period should be published alongside the equivalent statistics for previous recent periods. Where available, three or four year's worth of figures should be reported. Accountability Agents are encouraged to put some effort tin to clearly displaying and explaining the statistics so that stakeholders can better appreciate their significance. For example, clear tables of figures with accompanying graphs are helpful.

Q. *Are there steps that can be taken to facilitate comparison across APEC jurisdictions?*

A. Accountability Agents are to include a classification in their reported statistics based on the APEC information privacy principles. This will aid comparison. In classifying respondents to complaints by industry type, it is recommended that the International Standard Industrial Classification of All Economic Activities (revised by the United Nations in 2008) be used or national or regional standards on industry classification that are aligned with that international standard. (See http://unstats.un.org/unsd/cr/registry/regcst.asp?Cl=27&Lg=1

APEC CROSS-BORDER PRIVACY RULES SYSTEM PROGRAM REQUIREMENTS

The purpose of this document is to provide the baseline program requirements of the APEC Cross Border Privacy Rules (CBPR) System in order to assist APEC-recognized Accountability Agents in an Applicant's compliance review process and to ensure this process is conducted consistently throughout participating APEC Economies. Accountability Agents are responsible for receiving an Applicant's intake documentation, verifying an Applicant's compliance with the requirements of the CBPR System and, where appropriate, assisting the Applicant in modifying its policies and practices to meet the requirements of the CBPR System. The Accountability Agent will certify those Applicant deemed to have met the minimum criteria for participation provided herein, and will be responsible for monitoring the Participants' compliance with the CBPR System, based on this criteria. This document is to be read in consistently with the APEC CBPR Intake Document[1].

[1] *NOTE:* The APEC Cross Border Privacy Rules Intake Questionnaire lists the acceptable qualifications to the provision of notice, the provision of choice mechanisms, and the provision of access and correction mechanisms referred to in this document.

NOTICE

Assessment Purpose – *To ensure that individuals understand the applicant's personal information policies (subject to any qualifications), including to whom the personal information may be transferred and the purpose for which the personal information may be used. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of notice.*

Question	Assessment Criteria
1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.	If **YES,** the Accountability Agent must verify that the Applicant's privacy practices and policy (or other privacy statement) include the following characteristics: • Available on the Applicant's Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be specified). • Is in accordance with the principles of the APEC Privacy Framework; • Is easy to find and accessible. • Applies to all personal information; whether collected online or offline. • States an effective date of Privacy Statement publication. Where Applicant answers **NO to question 1**, and does not identify an applicable qualification subject to the Qualifications to Notice set out **below**, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.
1.a) Does this privacy statement describe how personal information is collected?	If **YES**, the Accountability Agent must verify that: • The statement describes the collection practices and policies applied to all covered personal information collected by the Applicant. • the Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and • The Privacy Statement reports the categories or specific sources of all categories of personal information collected. If **NO**, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle.
1.b) Does this privacy statement describe the purpose(s) for which personal information is	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to

collected?	individuals of the purpose for which personal information is being collected. Where the Applicant answers **NO** and does not identify an applicable qualification set out below, the Accountability Agent must notify the Applicant that notice of the purposes for which personal information is collected is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.
1.c) Does this privacy statement inform individuals whether their personal information is made available to third parties and for what purpose?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant notifies individuals that their personal information will or may be made available to third parties, **identifies the categories or specific third parties, and the purpose for which the personal information will or may be made available.** Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must notify the Applicant that notice that personal information will be available to third parties is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.
1.d) Does this privacy statement disclose the name of the applicant's company and location, including contact information regarding practices and handling of personal information upon collection? Where YES describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides name, address and a **functional** e-mail address. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that such disclosure of information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.
1.e) Does this privacy statement provide information regarding the use and disclosure of an individual's personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's Privacy Statement includes, if applicable, information regarding the use and disclosure of all personal information collected. Refer to question 8 for guidance on permissible uses of personal information. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant, that such information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.
1.f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Privacy Statement includes: • The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means). • The process that an individual must follow in order to correct his or her personal information Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent

	must inform the Applicant that providing information about access and correction, including the Applicant's typical response times for access and correction requests, is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.
2. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you provide notice that such information is being collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information is being (or, if not practicable, has been) collected **and that the notice is reasonably available to individuals**. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the notice that personal information is being collected is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.
3. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which personal information is being collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant explains to individuals the purposes for which personal information is being collected. The purposes must be communicated orally or in writing, for example on the Applicant's website, such as text on a website link from URL, attached documents, pop-up window, or other. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant of the need to provide notice to individuals of the purposes for which personal information is being collected. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.
4. Subject to the qualifications listed below, at the time of collection of personal information, do you notify individuals that their personal information may be shared with third parties?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant to provide notice to individuals that the personal information collected may be shared with third parties. Where the Applicant identifies an applicable qualification, the Accountability Agent must determine whether the applicable qualification is justified.

COLLECTION LIMITATION

Assessment 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 purposes may be a factor in determining what is relevant. In all instances, collection methods must be lawful and fair*

Question	Assessment Criteria
5. How do you obtain personal information: 5.a) Directly from the individual? 5.b) From third parties collecting on your behalf? 5.c) Other. If YES, describe.	The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information. Where the Applicant answers **YES to any of these sub-parts**, the Accountability Agent must verify the Applicant's practices in this regard. There should be at least one 'yes' answer to these three questions. If not, the Accountability Agent must inform the Applicant that it has incorrectly completed the questionnaire.
6. Do you limit your personal information collection (whether directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes?	Where the Applicant answers **YES** and indicates it only collects personal information which is relevant to the identified collection purpose or other compatible or related purposes, the Accountability Agent must require the Applicant to identify: • Each type of data collected • The corresponding stated purpose of collection for each; and • All uses that apply to each type of data • An explanation of the compatibility or relatedness of each identified use with the stated purpose of collection Using the above, the Accountability Agent will verify that the applicant limits the amount and type of personal information to that which is relevant to fulfill the stated purposes Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that it must limit the use of collected personal information to those uses that are relevant to fulfilling the purpose(s) for which it is collected.
7. Do you collect personal information (whether directly or through the use of third parties acting on your behalf) by lawful and fair	Where the Applicant answers **YES,** the Accountability Agent must require the Applicant to certify that it is aware of and complying with the requirements of the jurisdiction that governs the collection of such

means, consistent with the requirements of the jurisdiction that governs the collection of such personal information? Where YES, describe.	personal information and that it is collecting information by fair means, without deception. Where the Applicant Answers **NO**, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle.

USES OF PERSONAL INFORMATION

Assessment Purpose - *Ensuring that the use of personal information is limited to fulfilling the specific purposes of collection and other compatible or related purposes. This section covers use, transfer and disclosure of personal information. Application of this Principle requires consideration of the nature of the information, the context of collection and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" could extend, for example, to matters such as the creation and use of a centralized database to manage personnel in an effective and efficient manner; the processing of employee payrolls by a third party; or, the use of information collected by an applicant for the purpose of granting credit for the subsequent purpose of collecting debt owed to that applicant*

Question	Assessment Criteria
8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection, to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below.	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of written policies and procedures to ensure that] all covered personal information collected either directly or indirectly through an agent is done so in accordance with the purposes for which the information was collected as identified in the Applicant's Privacy Statement(s) in effect at the time of collection or for other compatible or related purposes. Where the Applicant Answers **NO**, the Accountability Agent must consider answers to Question 9 below.
9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below. 9.a) Based on express consent of the individual? 9.b) Compelled by applicable laws?	Where the Applicant answers **NO** to question 8, the Applicant must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the applicant selects 9a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained, and the Accountability Agent must verify that the Applicant's use of the personal information is based on express consent of the individual (9.a), such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify)

	Where the Applicant answers 9.a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 17-19 below. Where the Applicant selects 9.b, the Accountability Agent must require the Applicant to provide a description of how the collected personal information may be shared, used or disclosed as compelled by law. Where the Applicant does not answer 9.a or 9.b, the Accountability Agent must inform the Applicant that limiting the use of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.
10. Do you disclose personal information you collect (whether directly or through the use of third parties acting on your behalf) to other personal information controllers? If YES, describe. 11. Do you transfer personal information to personal information processors? If YES, describe. 12. If you answered YES to question 10 and/or question 11, is the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible or related purpose? If YES, describe.	Where the Applicant answers **YES** in questions 10 and 11, the Accountability Agent must verify that if personal information is disclosed to other personal information controllers or transferred to processors, such disclosure and/or transfer must be undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product requested by the individual, or compelled by law. Also, the Accountability Agent must require the Applicant to identify: 1) each type of data disclosed or transferred; 2) the corresponding stated purpose of collection for each type of disclosed data; and 3) the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.). Using the above, the Accountability Agent must verify that the Applicant's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or related purposes.
13. If you answered NO to question 12 or if otherwise appropriate, does the disclosure and/or transfer take place under one of the following circumstances? 13.a) Based on express consent of the individual?	Where applicant answers **NO** to question 13, the Applicant must clarify under what circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes. Where the Applicant answers **YES** to 13.a, the Accountability Agent must require the Applicant to provide a description of how individual's provide consent to having their personal information disclosed and/or transferred for an unrelated use, such as: • Online at point of collection

13.b) Necessary to provide a service or product requested by the individual? 13.c) Compelled by applicable laws?	• Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Applicant answers **YES** to 13.b, the Accountability Agent must require the Applicant to provide a description of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual. The Accountability Agent must verify that the disclosure or transfer is necessary to provide a service or product requested by the individual. Where the Applicant answers **YES** to 13.c, the Accountability Agent must require the Applicant to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement. Where the Applicant answers **NO** to 13.a, b and c, the Accountability Agent must inform the Applicant that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.

CHOICE

Assessment Purpose - *Ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information. However, this Principle recognizes, through the introductory words "where appropriate" in the Framework itself, that there are certain situations where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice. These situations are detailed in part II of the CBPR Self-Assessment Guidelines for Organisations. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of choice mechanisms.*

Question	Assessment Criteria
14. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of the mechanisms provided to individuals so that they may exercise choice in relation to the collection of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an applicable qualification the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.
15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of mechanisms provided to individuals so that they may exercise choice in relation to the use of their personal information, such as: • Online at point of collection • Via e-mail

	• Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be used. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent uses of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before:] • being able to make use of the personal information, when the purposes of such use is not related or compatible to the purpose for which the information was collected, and • Personal information may be disclosed or distributed to third parties, other than Service Providers. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification to the provision of choice, and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant a mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.
16. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of how individuals may exercise choice in relation to the disclosure of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and

	identify the purpose(s) for which the information will be disclosed. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent disclosures of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: • disclosing the personal information to third parties, other than Service Providers, for a purpose that is not related or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner , or compatible with that for which the information was collected.] Where the Applicant answers **NO**, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the disclosure of their personal information must be provided.
17 When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is displayed in a clear and conspicuous manner . Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clear and conspicuous in order to comply with this principle.
18. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is clearly worded and easily understandable. Where the Applicant answers **NO**, and/or when the Accountability Agent finds that the Applicant's choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clearly worded and easily understandable in order to comply with this principle.
19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is easily accessible and affordable. Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant that

personal information, are these choices easily accessible and affordable? Where YES, describe.	all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be easily accessible and affordable in order to comply with this principle.
20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.	Where the Applicant does have mechanisms in place, the Accountability Agent must require the Applicant to provide of the relevant policy or procedures specifying how the preferences expressed through the choice mechanisms (questions 14, 15 and 16) are honored. Where the Applicant does not have mechanisms in place, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not provide an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism to ensure that choices, when offered, can be honored, must be provided.

INTEGRITY OF PERSONAL INFORMATION

Assessment Purpose - *The questions in this section are directed towards ensuring that the personal information controller maintains the accuracy and completeness of records and keeps them up to date. This Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use*

Question	Assessment Criteria
21. Do you take steps to verify that the personal information held by you is up to date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use. **The Accountability Agent will verify that reasonable procedures are in place to allow the Applicant to maintain personal information that is up to date, accurate and complete, to the extent necessary for the purpose of use**. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.
22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use? Provide a description in the space below or in an attachment if necessary.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures and steps the Applicant has in place for correcting inaccurate, incomplete and out-dated personal information, which includes, but is not limited to, procedures which allows individuals to challenge the accuracy of information **such as accepting a request for correction from individuals by e-mail, post, phone or fax, through a website, or by some other method**. **The Accountability Agent must verify that this process is in place and operational.** Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures/steps to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.
23. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the transfer of the information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal information was transferred? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred and the accompanying procedures to ensure that the corrections are also made by the processors, agents or other service providers acting on the Applicant's behalf. The Accountability Agent must verify that these procedures are in place and operational, and that they effectively ensure that corrections are made by the processors, agents or other service providers acting on the Applicant's behalf.

	Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred, are required for compliance with this principle.
24. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the corrections to other third parties to whom the personal information was disclosed? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to other third parties, to whom personal information was disclosed. The Accountability Agent must verify that these procedures are in place and operational. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this principle.
25. Do you require personal information processors, agents, or other service providers acting on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed to ensure that personal information processors, agents, or other service providers to whom personal information was transferred inform the Applicant about any personal information known to be inaccurate incomplete, or outdated. The Accountability Agent will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being made by the Applicant and by the processors, agents or other service providers. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed, are required for compliance with this principle.

SECURITY SAFEGUARDS

Assessment Purpose - *The questions in this section are directed towards ensuring that when individuals entrust their information to an applicant, that applicant will implement reasonable security safeguards to protect individuals' information from loss, unauthorized access or disclosure, or other misuses*

Question	Assessment Criteria
26. Have you implemented an information security policy?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of this written policy. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.
27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include: • **Authentication and access control (eg password protections)** • **Encryption** • **Boundary protection (eg firewalls, intrusion detection)** • **Audit logging** • **Monitoring (eg external and internal audits, vulnerability scans)** • **Other (specify)** The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information and/or Third Party personal information it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access. Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held. The Applicant must take reasonable measures to require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.

	Where the Applicant indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.
28. Describe how the safeguards you identified in response to question 27 are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify that these safeguards are proportional to the risks identified. The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the personal information (whether collected directly from the individuals or through a third party) it gathers, in order to protect that information from unauthorized leakage, loss, use, alteration, disclosure, distribution, or access.
29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).	The Accountability Agent must verify that the Applicant's employees are aware of the importance of, **and obligations respecting**, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include: • Training program for employees • Regular staff meetings or other communications • Security policy signed by employees • Other (specify) Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.
30. Have you implemented safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held through: 30.a) Employee training and management or other safeguards? 30.b) Information systems and management, including network and software design, as well	Where the Applicant answers **YES** (to questions 30.a to 30.d), the Accountability Agent has to verify the existence each of the safeguards. The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant must employ suitable and reasonable means, such as encryption, to protect all personal information. Where the Applicant answers **NO** (to questions 30.a to 30.d), the Accountability Agent must inform the Applicant that the existence of safeguards on each category is required for compliance with this principle.

as information processing, storage, transmission, and disposal? 30.c) Detecting, preventing, and responding to attacks, intrusions, or other security failures? 30.d) Physical security?	
31. Have you implemented a policy for secure disposal of personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify the implementation of a policy for the secure disposal of personal information. Where the Applicant answers **NO**, the Accountability Agent must inform Applicant that the existence of a policy for the secure disposal of personal information is required for compliance with this principle.
32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures. Where the Applicant answers **NO,** the Accountability Agent must inform the Applicant that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this principle.
33. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 32? Describe below.	The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these tests.
34. Do you use **risk assessments or third-party certifications**? Describe below.	The Accountability Agent must verify that such **risk assessments or certifications** are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.
35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by: 35.a) Implementing an information security program that is proportionate to the sensitivity	The Accountability Agent must verify that the Applicant has taken reasonable measures (such as by inclusion of appropriate contractual provisions) to require information processors, agents, contractors, or other service providers to whom personal information is transferred, to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.

of the information and services provided? 35.b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of thepersonal information of the Applicant's customers? 35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?	

ACCESS AND CORRECTION

Assessment Purpose - *The questions in this section are directed towards ensuring that individuals are able to access and correct their information. This section includes specific conditions for what would be considered reasonable in the provision of access. Access will also be conditioned by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access. The details of the procedures whereby the ability to access and correct information is provided may differ depending on the nature of the information and other interests, which is why, in certain circumstances, it may be impossible, impracticable or unnecessary to change, suppress or delete records.*

The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right. While you should always make good faith efforts to provide access, in some situations, it may be necessary to deny claims for access and correction. Section II of the CBPR Self-Assessment Guidelines for Organisations sets out those conditions that must be met in order for such denials to be considered acceptable. When you deny a request for access, for the reasons specified herein, you should provide the requesting individual with an explanation as to why you have made that determination and information on how to challenge that denial. You would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of access and correction mechanisms.

Question	Assessment Criteria
36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place to respond to such requests. The Applicant must grant access to any individual, to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity. The Applicant's processes or mechanisms for access by individuals to personal information must be reasonable having regard to the manner of request and the nature of the personal information. The personal information must be provided to individuals in an easily comprehensible way. The Applicant must provide the individual with a time frame indicating when the requested access will be granted. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.
37. Upon request, do you provide individuals	Where the Applicant answers **YES** the Accountability Agent must verify each answer provided.

access to the personal information that you hold about them? Where YES, answer questions 37(a) – (e) and describe your applicant's policies/procedures for receiving and handling access requests. Where NO, proceed to question 38. 37.a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe. 37.b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe. 37.c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe. 37.d) Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc)? 37.e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.	The Applicant must implement reasonable and suitable processes or mechanisms to enable the individuals to access their personal information, such as account or contact information. If the Applicant denies access to personal information, it must explain to the individual why access was denied, and provide the appropriate contact information for challenging the denial of access where appropriate. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that it may be required to permit access by individuals to their personal information. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.
38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your applicant's policies/procedures in this regard below and answer questions 37 (a), (b), (c), (d) and (e). 38.a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in	Where the Applicant answers **YES to questions 38.a**, the Accountability Agent must verify that such policies are available and understandable in the primarily targeted economy. If the Applicant denies correction to the individual's personal information, it must explain to the individual why the correction request was denied, and provide the appropriate contact information for challenging the denial of correction where appropriate. All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the

the space below or in an attachment if necessary. 38.b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion? 38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion? 38.d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that the data has been corrected or deleted? 38.e) If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?	requesting individual. Where the Applicant answers **NO** to questions 38a-38e and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.

ACCOUNTABILITY

Assessment Purpose - *The questions in this section are directed towards ensuring that the Applicant is accountable for complying with measures that give effect to the other Principles stated above. Additionally, when transferring information, the Applicant should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.*

Question	Assessment Criteria
39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe. • Internal guidelines or policies (if applicable, describe how implemented) _____ • Contracts _____ • Compliance with applicable industry or sector laws and regulations ____ • Compliance with self-regulatory applicant code and/or rules ____ • Other (describe) ____	The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles.
40. Have you appointed an individual(s) to be responsible for your overall compliance with the Privacy Principles?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with these Principles. The Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with privacy principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of

	any remedial action where applicable. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that designation of such an employee(s) is required for compliance with this principle.
41. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to receive, investigate and respond to privacy-related complaints, such as: 1) A description of how individuals may submit complaints to the Applicant (e.g. Email/Phone/Fax/Postal Mail/Online Form); AND/OR 2) A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information; AND/OR 3) A formal complaint-resolution process; AND/OR 4) Other (must specify). Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.
42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to ensure individuals receive a timely response to their complaints. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.
43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.	The Accountability Agent must verify that the Applicant indicates what remedial action is considered.
44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints. Where the Applicant answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.
45. Do you have procedures in place for responding to judicial or other government	Where the Applicant answers **YES, the** Accountability Agent must verify that the Applicant has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that

subpoenas, warrants or orders, including those that require the disclosure of personal information?	require the disclosure of personal information, as well as provide the necessary training to employees regarding this subject. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.
46. Do you have mechanisms in place with personal information processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)? • Internal guidelines or policies _____ • Contracts _____ • Compliance with applicable industry or sector laws and regulations _____ • Compliance with self-regulatory applicant code and/or rules _____ • Other (describe) _____	Where the Applicant answers **YES, the** Accountability Agent must verify the existence of each type of agreement described. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such agreements is required for compliance with this principle.
47. Do these agreements generally require that personal information processors, agents, contractors or other service providers: • Abide by your APEC-compliant privacy policies and practices as stated in your Privacy Statement? _____ • Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement? _____ • Follow instructions provided by you relating to the manner in which your personal information must be handled?	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.

_____ • Impose restrictions on subcontracting unless with your consent? _____ • Have their CBPRs certified by an APEC accountability agent in their jurisdiction? _____ • Notify the Applicant in the case of a breach of the personal information of the Applicant's customers? • Other (describe) _____	
48. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.	The Accountability Agent must verify the existence of such self-assessments.
49. Do you carry out regular spot checking or monitoring of your personal information processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of the Applicant's procedures such as spot checking or monitoring mechanisms. Where the Applicant answers **NO**, the Accountability Agent must require the Applicant to describe why it does not make use of such spot checking or monitoring mechanisms.
50. Do you disclose personal information to other recipient **persons or organisations** in situations where due diligence and reasonable steps to ensure compliance with your APEC CBPRs by the recipient as described above is impractical or impossible?	If **YES**, the Accountability Agent must ask the Applicant to explain: (1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and (2) the other means used by the Applicant for ensuring that the information, nevertheless, is protected consistent with the APEC Privacy Principles. Where the Applicant relies on an individual's consent, the Applicant must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.

APEC CROSS-BORDER PRIVACY RULES SYSTEM

WORKPLAN FOR THE DEVELOPMENT OF A DIRECTORY OF CBPR CERTIFIED ORGANIZATIONS AND APEC-RECOGNIZED ACCOUNTABILITY AGENTS

Project Overview

1. The purpose of this project is to develop a publicly accessible directory of organizations that have been certified as compliant with the APEC Cross Border Privacy Rules (CBPR) System by APEC-recognized Accountability Agents.

2. This directory should be accessible from all participating APEC member economies. The development of a website to host this directory is considered the most cost-effective mechanism for such a directory. This website should comply with the APEC website guidelines and associated templates.

3. At a minimum, this directory should contain the following information:

- The relevant and up to date contact information for the certified organization;
- The relevant and up to date contact information for the APEC-recognized Accountability Agent used to certify that organization;
- The status of certification, including the date of certification;
- The relevant Privacy Enforcement Authority in the jurisdiction in which the organization is seeking certification;
- A link to the certified organization's website page that provides relevant information to the consumer about the organization's participation in the CBPR System, its privacy policies and practices, and complaint handling mechanisms; and
- Any information about an Economy's law and regulations relevant to privacy issues, including links to APEC IAPs.

4. This directory is intended to be an information resource for consumers. It is the responsibility of the certified organization and the relevant Accountability Agent to make information available on the complaint handling process.

5. The information contained in this directory is intended to be one of multiple entry points for a consumer into the CBPR system. A consumer may also obtain information directly from certified organizations, from the appropriate government agencies or public authorities in their economy, or from APEC itself. In addition to this directory, participating APEC economies may wish to develop and maintain their own websites containing additional information related to the CBPR system.

Directory Management

6. Each participating APEC economy will designate a contact point to collect all relevant information for CBPR-certified organizations and APEC-recognized Accountability Agents within their economy. It is the responsibility of the certified organization and Accountability Agent to ensure that all information provided to the contact point is up to date and accurate.

7. The designated contact point will forward all collected information to the appropriate website administrator for inclusion on the website.

8. Organizations will only be listed in the directory after they have been certified as compliant with the minimum requirements of the CBPR system by an APEC-recognized Accountability Agent. Should they cease participation in the CBPR system for any reason, they will be removed from the website. The listing of an Accountability Agent will only occur after they have been recognized by APEC member economies and only as long as such recognition lasts.

9. As part of the implementation of this project, a process will be developed to ensure the maintenance and review of the information contained in the directory by participating APEC economies.

Website Development and Maintenance

10. Hosting: The Directory should be hosted on an APEC website and subject to the requirements and policies of the APEC Secretariat[1].

11. Costs: There are costs associated in the development and maintenance of the website. It is not possible for the APEC Secretariat to meet these costs. These costs will need to be addressed as part of the broader implementation of the CBPR system.

Additional Functions

12. The website may be expanded at the discretion of APEC economies and the APEC Secretariat to provide a comprehensive range of information and services regarding additional elements of the CBPR system for both stakeholders and participants. Services to be provided could include an automated technical assistance tool to help organizations develop complaint-handling privacy rules.

[1] [1] http://webresources.apec.org/

WEBSITE DEVELOPMENT WORK PLAN

A. Planning

1. Consider the proposed content for the website
2. Creation of a website objectives document that articulates the goals of the website
3. Creation of a maintenance plan detailing how content will be updated and the process and frequency of such updates
4. Creation of a project brief, describing the entirety of the project
5. Consultation with relevant stakeholders, including organizations and consumer representatives, on the useful content of the website
6. Determine outside sponsorship, if necessary, and conformity with the APEC Sponsorship Guidelines: http://www.apec.org/etc/medialib/apec_media_library/downloads/som/pubs.Par.0001.File.v1.1

B. Development

1. Conduct systems analysis of the project brief
2. Determine technical and functional specifications based on the systems analysis
3. Design iBoards (diagrams illustrating functional specifications)
4. Programming (coding of the website)
5. Create website policies on how the website is to be managed and administered
6. Targeted consultation with stakeholders

C. Testing

1. Create test environment (how testing is to be done and who will be involved)
2. Create a 'Test Cases Document' detailing the steps that testers are to take. Tests are to cover the functionalities on the website.
3. Test Exercise based on test cases documentation.

D. Deployment

1. Soft launch for a limited group to access and conduct a final test
2. Receive approval for 'APEC Website Status' and use of APEC Logo
3. Deploy

REQUEST FOR CONTACT POINT INFORMATION FORM

Explanatory Notes

Contact Point Collection Form

This document is used by certified organizations and APEC-recognized Accountability Agents to submit their contact details to the appropriate government entity in their economy for inclusion in a directory of CBPR certified organizations. The contact point collection form is attached.

Purpose of the Directory

The purpose of the directory is to serve as an entry point mechanism for consumers to access information about the CBPR system, check the accreditation of participating organizations, access the privacy policies and practices of accredited organizations, and to lodge complaints.

Role of the Contact Point

The contact point is an organization's first point of contact for consumers seeking information about the organization's participation in the CBPR System or lodging a complaint in relation to personal information to which the CBPR system applies. The contact point is, on behalf of the organization, accountable for the organization's compliance with its business privacy rules and the requirements of the CBPR System.

Contact Point information from Accountability Agents

The directory will also contain contact information for accountability agents. The purpose of collecting this information is to assist consumers in making contact with accountability agents. The Contact Point Form asks organizations to identify their accountability agent (if any). This information will be included in the listing for an organization, allowing consumers to directly contact the relevant accountability agent if they wish to lodge a complaint.

CBPR SYSTEM CONTACT POINT DESIGNATION FORM

ORGANIZATION	
APEC MEMBER ECONOMY	
CONTACT POINT NAME, TITLE/POSITION	
E-MAIL	
TELEPHONE	
FAX	
RELEVANT WEBSITE ADDRESS	
PHYSICAL ADDRESS	
CERTIFYING ACCOUNTABILITY AGENT	
ACCOUNTABILITY AGENT CONTACT POINT NAME	
ACCOUNTABILITY AGENT CONTACT POINT EMAIL	
ACCOUNTABILITY AGENT CONTACT POINT ADDRESS	
DATE OF CERTIFICATION	
DATE OF SUBMISSION OF FORM	

Privacy Notice: *This information is being collected for the purpose of compiling a directory of contact points in certified organizations and APEC-recognized Accountability Agents in those APEC economies participating in the APEC Cross-Border Privacy Rules System. The information collected will be publicly available. Contact points may also be contacted as a group to communicate general information, updates and for the purposes of consultation.*

APEC COOPERATION ARRANGEMENT FOR CROSS-BORDER PRIVACY ENFORCEMENT

1 OBJECTIVES OF THIS FRAMEWORK

In endorsing the APEC Privacy Framework in 2004, APEC leaders recognised the importance of developing effective privacy protections that avoid barriers to information flows and ensure continued trade and economic growth in the APEC region.[1] This cross-border cooperation arrangement is a key step in achieving that goal.

The APEC Privacy Framework, Part IVB, calls on member economies to consider developing cooperative arrangements and procedures to facilitate cross-border cooperation in the enforcement of privacy laws. The APEC Privacy Framework contemplated bilateral or multilateral arrangements that include the following:

- mechanisms for promptly, systematically and efficiently notifying designated public authorities in other member economies of investigations or privacy enforcement cases that target unlawful conduct or the resulting harm to individuals in those economies;
- mechanisms for effectively sharing information necessary for successful cooperation in cross-border privacy investigation and enforcement cases;
- mechanisms for investigative assistance in privacy enforcement cases;
- mechanisms to prioritize cases for cooperation with public authorities in other economies based on the severity of the unlawful infringements of personal information privacy, the actual or potential harm involved, as well as other relevant considerations; and
- steps to maintain the appropriate level of confidentiality in respect of information exchanged under the cooperative arrangements.[2]

In addition, in 2007, APEC economies endorsed a 'pathfinder' for international implementation of the APEC Privacy Framework. The Cooperation Arrangement for Cross-border Privacy Enforcement is one outcome of the Pathfinder. The Pathfinder also seeks to facilitate development of a framework for accountable flows of personal information across borders, focussing on the use of Cross-Border Privacy Rules by

[1] *APEC Privacy Framework*, available at http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1

[2] Part IV, *APEC Privacy Framework*, available at http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1

business. The Pathfinder aims to support this cross-border privacy rules system with a framework for cross-border cooperation in the enforcement of information privacy.[3]

In 2007, the Organization for Economic Cooperation and Development (OECD) adopted a recommendation to promote cooperation between Member countries on the enforcement of laws protecting privacy.[4]

In light of this background, the goals of this Cooperation Arrangement are to:

- facilitate information sharing among Privacy Enforcement Authorities in APEC economies;
- establish mechanisms to promote effective cross-border cooperation between Privacy Enforcement Authorities on the enforcement of Privacy Law, including through referrals of matters and through parallel or joint investigations or enforcement actions;
- facilitate Privacy Enforcement Authority cooperation in enforcing Cross-Border Privacy Rules; and
- encourage information sharing and cooperation on privacy investigation and enforcement with privacy enforcement authorities outside APEC, including by ensuring this Cooperation Arrangement can work seamlessly with similar arrangements such as those developed under the OECD Recommendation.

2 OUTLINE OF THIS COOPERATION ARRANGEMENT

2.1 This Cooperation Arrangement creates a practical multilateral mechanism for Privacy Enforcement Authorities to cooperate in cross-border privacy enforcement. It does this by creating a framework under which Privacy Enforcement Authorities may, on a voluntary basis, share information and request and render assistance in certain ways.

2.2 Any Privacy Enforcement Authority in an APEC economy may participate in this Cooperation Arrangement.

2.3 An Economy can have more than one participating Privacy Enforcement Authority provided each public body meets the criteria established in the definition of Privacy Enforcement Authority as contained in paragraph 4.1.

[3] *APEC Data Privacy Pathfinder* (2007) available at http://aimp.apec.org/Documents/2007/SOM/CSOM/07_csom_019.doc.

[4] Organisation for Economic Cooperation and Development, (2007) *Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy, available at: www.oecd.org/dataoecd/43/28/38770483.pdf.*

2.4 This Cooperation Arrangement is set out as follows:

- commencement of this Cooperation Arrangement (paragraph 3);
- definitions and legal limitations (paragraphs 4, 6 and 7);
- the role of the Administrator (paragraph 5);
- how to participate, or cease to participate, in the Cooperation Arrangement (paragraph 8);
- cross-border cooperation (paragraph 9);
- confidentiality (paragraph 10);
- information sharing (paragraph 11); and
- miscellaneous matters (staff exchanges, disputes, review) (paragraphs 12 to 15).

2.5 Annexed to the Cooperation Arrangement are:

- Request for Assistance form (Annex A).
- Contact Point Designation form (Annex B).
- A template for summary statement of Participant's practices, policies and activities (Annex C).

3 COMMENCEMENT

3.1 This Cooperation Arrangement commences one month after the Administrator is designated under paragraph 5 or such later date specified by the ECSG.

3.2 From the date of commencement any Privacy Enforcement Authority may participate in the Cooperation Arrangement as provided for in paragraph 8.

4 DEFINITIONS

4.1 In this Cooperation Arrangement:

'**Administrator'** means the body or bodies designated under paragraph 5.1.

'**Cooperation Arrangement**' means APEC Cooperation Arrangement for Cross-border Privacy Enforcement.

'Cross-Border Privacy Rules' has the same meaning as in paragraphs 46 to 48 of the APEC Privacy Framework.

'**ECSG**' means the Electronic Commerce Steering Group or the APEC committee having responsibility for the APEC Privacy Framework.

'**Participant**' means a Privacy Enforcement Authority from an APEC member economy that participates in this Cooperation Arrangement.

'**Privacy Enforcement Authority**' means any public body that is responsible for enforcing Privacy Law, and that has powers to conduct investigations or pursue enforcement proceedings.

'**Privacy Law**' means laws and regulations of an APEC economy, the enforcement of which have the effect of protecting personal information consistent with the APEC Privacy Framework.

'**Receiving Authority**' means a Participant that has received a "Request for Assistance" from another Participant.

'**Request for Assistance**' includes, but is not limited to:

(i) a referral of a matter related to the enforcement of a Privacy Law;

(ii) a request for cooperation on the enforcement of a Privacy Law;

(iii) a request for cooperation on the investigation of an alleged breach of a Privacy Law; and

(iv) a transfer of a privacy complaint.

'**Requesting Authority**' means a Participant that has made a Request for Assistance of another Participant.

5 ROLE OF THE COOPERATION FRAMEWORK ADMINISTRATOR

5.1 The ECSG will designate:

(i) the APEC Secretariat; or

(ii) a Privacy Enforcement Authority (with its consent); or

(iii) the APEC Secretariat and a Privacy Enforcement Authority (with its consent) jointly

to perform the functions of the Administrator.

5.2 The designation under paragraph 5.1 may be for a limited duration and may be revoked or altered by the ECSG at any time. In the event that a Privacy Enforcement Authority designated as the Administrator ceases to be so designated (through expiry, revocation, resignation or through ceasing to be a Privacy Enforcement Authority) the APEC Secretariat will perform the core functions of the Administrator pending any new designation (and may perform any of the additional functions).

5.3 The Administrator will perform the following core functions:

(i) receive:

(a) notices of intent to participate in or cease to participate in the Cooperation Arrangement under paragraphs 8.1 and 8.2;

(b) letters of confirmation under paragraph 8.1;

(c) economy contact point forms, under paragraph 11.1;

(ii) receive such documents in paragraph 5.3(i) and verify that the participating authority is a Privacy Enforcement Authority as defined in this Cooperation Arrangement;

(iii) subject to the outcome of paragraph 5.3(ii), arrange for documents received under paragraph 5.3(i)(a) and (c) to be made available through the APEC website or other appropriate accessible means;

(iv) maintain and make available:

(a) an up-to-date list of current subscribers;

(b) a compilation of economy contact points;

(v) review the operation of the Cooperation Arrangement three years after its commencement as set out in paragraph 15;

5.4 The Administrator may also perform the following additional functions:

(i) publicise the Cooperation Arrangement in conjunction with APEC, member economies and stakeholders;

(ii) publish a directory of any bodies, whether or not Privacy Enforcement Authorities or participants, having a role to play in the protection of privacy;

(iii) promote initiatives to support cooperation amongst Participants through, for instance, teleconferences, seminars, staff exchanges, and cooperation with other enforcement networks;

(iv) facilitate exploring, recording and reviewing common enforcement priorities.

6 CHARACTER OF THIS DOCUMENT

6.1 This arrangement is to be read consistently with the APEC Privacy Framework.

6.2 Nothing in this Cooperation Arrangement is intended to:

(i) Create binding obligations, or affect existing obligations under international or domestic law, or create obligations under the laws of the Participants' economies.

(ii) Prevent a Participant from seeking assistance from or providing assistance to another Participant or another non-participating enforcement authority of an APEC member economy, pursuant to other agreements, treaties, arrangements, or practices.

(iii) Affect any authority or right of a Privacy Enforcement Authority or non-participating authority to seek information on a lawful basis, including in law enforcement matters, from a person located in the territory of another Participant's economy, nor is it intended to preclude any such person from voluntarily providing information to a Privacy Enforcement Authority or non-participating authority.

(iv) Impede governmental activities authorized by law when taken to protect security, public safety, sovereignty or other public policy of an APEC member economy.

(v) Create obligations or expectations of cooperation that would exceed a Participant's scope of authority and jurisdiction.

(vi) Create obligations or expectations for other, non-participating government agencies.

(vii) affect any authority or right to use information pursuant to a mutual legal assistance treaty (MLAT) or other applicable international agreements between the Requesting and Receiving Authorities' governments.

7 LIMITATIONS ON ASSISTANCE

7.1 At its sole discretion, a Participant may at any time decline to accept or proceed with a Request for Assistance, or limit its cooperation including, but not limited, under the following circumstances:

(i) The matter is inconsistent with domestic law or policy.

(ii) The matter is not within the Participant's scope of authority or jurisdiction.

(iii) The matter is not an act or practice of a kind that both the Requesting Authority and Receiving Authority are authorized to investigate or enforce against under their Privacy Laws.

(iv) There are resource constraints.

(v) The matter is inconsistent with other priorities.

(vi) There is an absence of mutual interest in the matter in question.

(vii) The matter is outside the scope of this Cooperation Arrangement.

(viii) Another body (including a private sector body, consistent with paragraph 9.4) is a more appropriate body to handle the matter.

(ix) Any other circumstances that renders a Participant unable to cooperate. The Participant may notify the basis of these circumstances in writing.

8 PARTICIPATING IN THE COOPERATION ARRANGEMENT

8.1 A Privacy Enforcement Authority may participate in this Cooperation Arrangement by giving written notice to the Administrator. The participation should be supported by a written letter of confirmation from the economy's ECSG delegation, or other appropriate governmental representative, that the applicant is a Privacy Enforcement Authority within the meaning of the definition in paragraph 4.1. The participation will take effect after the Administrator has formally accepted the Participant's written notice, subject to the outcomes of paragraph 5.3(ii).

8.2 A Participant may cease participation in this Cooperation Arrangement by giving one month's written notice to the Administrator.

8.3 A Privacy Enforcement Authority should, as soon as reasonably practicable after notifying the Administrator under paragraphs 8.1 or 8.2, take reasonable steps to make the participation or cessation of participation known to other Participants. This should include posting information on the Authority's website during the period it has participated in the Cooperation Arrangement and for a reasonable period after ceasing to participate.

8.4 A Privacy Enforcement Authority planning to cease participation in the Cooperation Arrangement that has received, or is currently acting upon, a Request for Assistance should consider whether it will be able to fulfil what is expected of it under this Cooperation Arrangement in relation to the request after it has ceased participation. If the request will be affected, the Authority should exercise its best endeavour to protect the interests of the Requesting Authority and the individuals concerned and ensure that they are advised of, or consulted upon, any actions to be taken.

9 CROSS-BORDER COOPERATION

Cross-border cooperation on enforcement of Privacy Law

9.1 Subject to paragraphs 6 and 7, Participants should assist one another by considering other Participants' Requests for Assistance and referrals for investigation or enforcement, and share information and cooperate on the investigation or enforcement of Privacy Laws.

Prioritisation of matters for cross-border cooperation

9.2 Given that cross-border cooperation can be complex and resource-intensive, Participants may individually or collectively prioritize those matters that are most serious in nature based upon the severity of the unlawful infringements of personal information privacy, the actual or potential harm involved, as well as other relevant considerations. Participants requesting prioritisation of a particular Request for Assistance should specify the reasons in the Request for Assistance form.

9.3 Subject to paragraphs 7.1 and 9.2, Participants recognize the enforcement of APEC Cross-Border Privacy Rules as a priority for cooperation under this Arrangement.

Cooperation with non-participating agencies and organisations

9.4 Participants intend to use best efforts within the limits of their respective authority to cooperate with private sector organizations, self-regulatory bodies and non-participating Privacy Enforcement Authorities, whose responsibilities include the resolution of individuals' privacy complaints. Privacy Enforcement Authorities are in particular encouraged to cooperate with Accountability Agents involved in the enforcement of APEC Cross-Border Privacy Rules.

9.5 Participants intend to use best efforts within the limits of their respective authority to cooperate with other public sector bodies including law enforcement bodies, subject to paragraph 10.

Steps prior to requesting assistance

9.6 Before a Participant makes a Request for Assistance to another Participant, that Participant should:

(i) ascertain that the request would be consistent with this Cooperation Arrangement and the goals of the APEC Privacy Framework;

(ii) seek consent, where appropriate and subject to any other requirements, policies or practices applicable to the Privacy Enforcement Authority in question, of individual complainants to provide information about their complaint to another Participant;

(iii) check the accessible information on the other Participant's practices, policies and activities (see paragraphs 11.2 and 11.3);

(iv) perform a preliminary enquiry, where appropriate and practicable, to identify which entity in the other member economy has front-line responsibility with respect to the contemplated Request for Assistance consistent with paragraphs 9.4 and 9.5; and

(v) perform a preliminary enquiry, where appropriate, with the contact point (designated under paragraph 11.1) of the other Participant or other appropriate entity in the other member economy and provide information as necessary, to identify if the other Participant will have and accept jurisdiction over the contemplated Request for Assistance.

Requesting assistance

9.7 A Participant making a Request for Assistance to another Participant should:

(i) use the APEC 'Request for Assistance' form (attached at Annex A) to communicate key information about the matter in question;

(ii) provide sufficient additional information (if any) for the Receiving Authority to take action, such as identifying any special precautions that should be taken in the course of fulfilling the request;

(iii) specify the purpose for which any information requested from the Receiving Authority will be used and the persons to whom the information may be transferred; and

(iv) provide information, or other assistance, requested by the Receiving Authority to assist with the handling of the referred matter.

9.8 A Participant whose assistance is requested should:

(i) acknowledge the Request for Assistance as soon as reasonably practicable after receiving it;

(ii) at the time of acknowledgement, or as soon as reasonably practicable thereafter, indicate whether it accepts or declines the request in whole or in part;

(iii) if more information is needed from the Requesting Authority to enable a decision to be made on accepting or declining the request, promptly identify that further information is required and to clearly advise the Requesting Authority of this;

(iv) if declining the Request for Assistance, provide the reason(s) for such a decision and refer the Requesting Authority, where feasible and appropriate, to a body which may be able to handle the request (consistent with paragraphs 9.4 and 9.5);

(v) if limiting the extent of cooperation, provide the reason(s) for such decision and advise any condition(s) to be imposed for rendering assistance; and

(vi) if accepting the Request for Assistance:

(a) process that request according to its usual policy and practice;

(b) where feasible and appropriate, communicate with the Requesting Authority about matters that may assist with the processing of the matter in question; and

(c) where feasible and appropriate, keep the Requesting Authority informed of the progress and outcome of the referred matter.

Communication to assist ongoing investigations

9.9 Participants should communicate with each other, as appropriate, about matters that may assist ongoing investigations.

Use of information obtained during cross-border cooperation

9.10 The Requesting Authority and the Receiving Authority will, on a bilateral basis, determine permissible uses of shared information consistent with applicable law and policy.

Notice of possible breaches in another Participant's jurisdiction

9.11 A Participant may, if it considers appropriate, provide another Participant with notice of a possible breach of the privacy laws of that other Participant's economy.

9.12 Where appropriate and feasible, Participants should coordinate their investigations and enforcement activity with that of other Participants to promote more effective enforcement and avoid interference with ongoing investigations.

10 CONFIDENTIALITY

10.1 Subject to paragraphs 9.10 and 10.3, and in accordance with any laws applicable to the Requesting and Receiving Authority, consultations, other communications or information shared between Participants pursuant to this Cooperation Arrangement, are confidential and will not be disclosed.

10.2 Each Participant should, to the fullest extent possible and consistent with its economy's laws, use best efforts to maintain the confidentiality of any information communicated to it in confidence by another Participant and respect any safeguards sought by the other Participant.

10.3 Nothing in this Cooperation Arrangement prevents disclosure of confidential information to third parties, such as other law enforcement agencies, if such disclosure is required by the law of the Requesting Authority's economy. Participants should state clearly all likely requirements for disclosure in their statements of practices, policies and activities (see paragraphs 11.2 and 11.3) and an updated statement of practices, policies and activities should accompany a Request for Assistance when seeking confidential information from another Participant. Where a Requesting Authority is subject to a legal requirement to disclose, it should use best efforts to notify the Receiving Authority at least ten days in advance of any such proposed disclosure or, if such notice cannot be given, then as promptly as possible.

10.4 Confidential information disclosed under paragraphs 10.3 and 9.10 should be subject to appropriate confidentiality assurances.

10.5 Upon ceasing participation in this Cooperation Arrangement, a Privacy Enforcement Authority should maintain the confidentiality of any information provided to it in confidence by another Participant. Any information provided under the Cooperation Arrangement should be held securely and confidentially, returned

or otherwise handled in accordance with the consent of the Participant that provided it.

10.6 Subject to paragraphs 9.10 and 10.3, Participants intend to oppose, to the fullest extent possible consistent with their economies' laws, any application by a third party for disclosure of confidential information or materials received from other Participants, subject to consultation with the Participants that provided the information.

10.7 Each Participant should endeavour to safeguard the security of any information received under this Cooperation Arrangement. To this effect, a Participant should have in place appropriate measures to prevent loss, unauthorized or accidental access, processing, use or disclosure of any information received under this Cooperation Arrangement. Any information received under this Cooperation Arrangement should not be retained for longer than required by domestic law or than is necessary for the fulfillment of the purpose for which the information is to be used.

11 INFORMATION SHARING

Contact point designation

11.1 Each Participant should designate a contact for the purposes addressed in this Cooperation Arrangement and as the main, but not exclusive, point of contact for other Privacy Enforcement Authorities. The Contact Point Designation form (or an updated version provided for this purpose by the Administrator) annexed to this Cooperation Arrangement may be used.

Participants' statement of practices, policies and activities

11.2 Participants should prepare a statement of information related to their enforcement practices and policies and other relevant activities. Participants should take steps to make this statement accessible to other Participants, for example, by posting it on their website. Availability of these statements will improve Participants' collective understanding of how enforcement is conducted within respective economies as well as assisting in the facilitation of particular Requests for Assistance.

11.3 The Administrator may request Participants to file summary statements of enforcement practices to be available to Participants in a central repository. If doing so, the Administrator will use the template annexed to this Cooperation Arrangement or an updated version of that template. Participants should provide the Administrator with an updated summary within a reasonable time frame if their policies or practices change.

Sharing of experiences

11.4 Each Participant is encouraged, where feasible and appropriate, to provide information in their possession to other Participants respecting important developments in relation to matters within the scope of this Cooperation Arrangement, including:

(i) surveys of public attitudes bearing upon enforcement matters;

(ii) details of research projects having an enforcement or cross-border cooperation dimension;

(iii) enforcement training programmes;

(iv) changes in relevant legislation;

(v) experiences with various techniques in investigating privacy violations and with regulatory strategies, including self-regulatory strategies, involving such violations;

(vi) information about trends and developments in the types and numbers of complaints and disputes they handle; and

(vii) opportunities for privacy enforcement staff training and employment.

12 STAFF EXCHANGES

12.1 Participants may explore bilateral opportunities to arrange secondments of staff or staff exchanges or enable specialist staff to assist other Participants in particular matters.

12.2 Participants may also, where appropriate, consider the feasibility of:

(i) enabling staff to participate in training programmes that another Participant is conducting;

(ii) developing joint training programmes;

(iii) sharing specialist training resources.

13 COSTS

13.1 Each Participant bears their own costs of providing information or assistance in accordance with this Cooperation Arrangement and in otherwise cooperating as contemplated by this Cooperation Arrangement.

13.2 Participants may negotiate to share or transfer costs of responding to a specific Request for Assistance, offer of training, or other cooperation.

14 DISPUTES

14.1 Any dispute between Participants in relation to this Cooperation Arrangement is to be resolved by discussions between them through their designated contacts and, failing resolution in a reasonably timely manner, by discussion between the heads of the Participants.

15 REVIEW AND UPDATE OF THIS DOCUMENT

15.1 Through a consultative process, Participants must review this Cooperation Arrangement and its operation three years after its commencement.

15.2 Having completed the review, the Administrator will submit a report to the ECSG giving an account of the review and offering recommendations of any necessary or desirable changes.

15.3 The Administrator will manage a process for soliciting and receiving acceptances from Participants of the changes approved by the ECSG and will appropriately update the list of current Participants and make the revised Cooperation Arrangement available.

Request for Assistance Form

Please see the instructions below

Date of the request:

1. Case name

2. Authority contact details

From:

Requesting Authority, Economy	
Contact Person, Title	
Telephone	
Email Address	
Postal address	

To:

Receiving Authority, Economy	
Contact Person, Title	
Telephone	
Email Address	
Postal address	

3. Confidentiality requirements

4. Assistance requested

5. Time and manner of response

6. Organization(s) involved

Name	
Address/URL	
Contact Person, Title	
Telephone/ Email Address	
Principal Activities	
Any additional background information:	

7. Individual(s) involved

Name	
Address	
Telephone/ Email Address	
Any additional background information:	

8. Background and status of the investigation

9. Type of Privacy Principles at Issue

You may add explanation under each principle if necessary.

	Yes	No
Preventing harm *(APEC Privacy Principle 1)* [*e.g.* risk of harm that may result from the misuse of personal information]		
Notice (*APEC Privacy Principle 2*) [*e.g.* notification of, and information on, the existence of data processing]		
Collection Limitation (*APEC Privacy Principle 3*) [*e.g.* personal information collected is limited to information that is relevant to the stated purposes of collection; has been obtained by lawful and fair means; and, where appropriate, with notice to, or consent of, the individual concerned]		
Uses of Personal Information (*APEC Privacy Principle 4*) [*e.g.* personal information only used only to fulfill the purposes of collection and/or related purposes except: with the consent of the individual whose personal information is collected; when necessary to provide a service/product requested by the individual; or, by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.]		

Choice (*APEC Privacy Principle 5*) [*e.g.* the provision of clear, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of a individual's personal information, where appropriate].		
Integrity of Personal Information (*APEC Privacy Principle 6*) [*e.g.* personal information is accurate, complete and kept up-to-date to the extent necessary for the purposes of use.]		
Security Safeguards (*APEC Privacy Principle 7*) [*e.g.* personal information controllers have used the appropriate administrative, technical or procedural mechanisms for insuring the confidentiality, integrity, and protection of data.]		
Access and Correction (*APEC Privacy Principle 8*) [*e.g.* individuals are able to: obtain confirmation of whether or not the personal information controller holds personal information about them; challenge the accuracy and, if possible have the information rectified, completed, amended or deleted, where possible.]		
Accountability (*APEC Privacy Principle 9*) [*e.g.* personal information controller is accountable for complying with measures that give effect to the APEC Privacy Principles, including		

when transferring personal information domestically or internationally.]		

10. Possible law violations, potential sanctions, on-going proceedings and contemplated proceedings

11. Other Relevant Information

Instructions

1. Case name

Provide a name, number or other indication that can be used to refer to the request.

2. Authority contact details

Provide the contact details specified in the form for the Requesting Authority and the Receiving Authority. Where appropriate, provide contact information for any other Authorities (domestic or foreign) that have been involved in the investigation or whose assistance has been requested, to help ensure effective co-ordination.

APEC maintains a directory of Privacy Enforcement Authorities. The directory may assist in the identification of Privacy Enforcement Authorities in another economy. To access this directory conditions apply. Please contact **(insert instructions based on outcome of project 5)**.

3. Confidentiality requirements

Indicate what confidentiality requirements are requested of the Receiving Authority. For some requests, assurances regarding confidentiality may be needed prior to transmitting this Request for Assistance (which will likely contain the information for which confidential treatment is required). Requesting Authorities can contact the Receiving Authority in advance to specify and obtain agreement on the confidentiality requirements. In addition, indicate any special instructions as to how the information provided should be handled (*e.g.* whether the individuals or organizations concerned can be contacted).

4. Assistance requested

Describe the type of information needed or other type of assistance sought and indicate why the information will be of assistance.

5. Time and manner of response

Indicate the preferred manner in which the response/information is to be transmitted (*e.g.* telephone, email, courier, computer disk) as well as any deadlines by which the information is needed. If there are any special evidentiary or procedural requirements that should be observed by the Receiving Authority these could be noted as well. Describe reasons for why the Request for Assistance should be given priority.

6. Organization(s) involved

Identify the organization involved in the request, including its contact details and information about its principal activities. As needed, copy and complete the table for other organizations or agents involved.

7. Individual(s) involved

Identify or describe the individual(s) whose personal information is at issue. As needed, copy and complete the table for other individuals whose personal data is at issue.

8. Background/Status

Provide a short summary of the background and current status of the investigation. This summary should include relevant background facts underlying the investigation. Possible issues to mention could include, *e.g.*, the date and description of key activities, investigative avenues already pursued, whether there has been any attempt by the individual to seek redress from the organisation or an accountability agent and key facts that give rise to the cross-border dimension.

9. Type of privacy principles at issue

Indicate whether the subject matter of the Request relates to any of the privacy principles described in the table. You may add an explanation under each principle if necessary.

10. Possible law violations, potential sanctions, on-going proceedings and contemplated proceedings

Where appropriate, indicate the possible laws or regulations that may have been violated, the possible sanctions that could be applied, as well as information on any on-going and contemplated proceedings. Note that links to the full texts of national laws should be available elsewhere, but that some description or citation to the relevant provisions may be useful to the Receiving Authority in determining how to respond to the Request.

11. Other relevant information

Provide any additional information that may be helpful in responding the Request.

Contact Point Designation Form

Economy Name: _____ Date: _____

Contact Point

Please provide information for each category. This information will be maintained in a non-public list.

Privacy Enforcement Authority	
Name	
Title/Position	
Address	
Telephone	
Fax	
E-mail	
Website address	

(Optional) Other Privacy Enforcement Authorities in your economy and their website addresses	

Summary statement of Privacy Enforcement Authority enforcement practices, policies and activities

This form seeks to capture in summary form the enforcement jurisdiction and policies of each Participant in the APEC Cooperation Arrangement for Cross-Border Privacy Enforcement. The information will usually be posted on the relevant Participant's website and, when available, at a central reference point maintained by the Administrator.

Privacy Enforcement Authority name:

Economy:

Website address:

Key law(s) enforced by your authority:

(Consider including a link to the relevant legislation)

General sectors/jurisdictions regulated by your authority:

(Public sector, private sector, a particular industry sector? Do you operate in a particular geographical jurisdiction such as a state or province?)

Approach to investigation / resolution of enforcement matters:

(What are your key enforcement activities or roles? For example, do you receive complaints, grant approvals, investigate, mediate or make determinations on matters? Broadly speaking, what are your investigation processes? What are your enforcement powers?)

Prioritization policies:

(Does your authority have a policy on the prioritization of enforcement matters it is willing to handle? If so, please provide a link to your current policy)

Other relevant information:

(Are there any restrictions on how your agency can cooperate on enforcement? Are there any circumstances in which your agency may be required by law to provide information obtained under the Cooperation Arrangement to a third party?)

APEC CROSS-BORDER PRIVACY RULES SYSTEM

POLICIES, RULES AND GUIDELINES

The purpose of this document is to describe the APEC Cross Border Privacy Rules (CBPR) System, its core elements, governance structure and the roles and responsibilities of participating organizations, Accountability Agents and Economies. This document is to be read consistently with the APEC Privacy Framework. Nothing in this document is intended to create binding international obligations, affect existing obligations under international or domestic law, or create obligations under the laws and regulations of APEC Economies.

DEVELOPMENT OF THE CBPR SYSTEM

1. APEC plays a critical role in the Asia Pacific region by promoting a policy framework designed to ensure the continued free flow of personal information across borders while establishing meaningful protection for the privacy and security of personal information.

2. In November 2004, Ministers for the twenty-one APEC Economies endorsed the APEC Privacy Framework[1]. The Framework is comprised of a set of nine guiding principles and guidance on implementation to assist APEC Economies in developing consistent domestic approaches to personal information privacy protections. It also forms the basis for the development of a regional approach to promote accountable and responsible transfers of personal information between APEC Economies.

3. The Privacy Framework provides "a principles-based … framework as an important tool in encouraging the development of appropriate information privacy protections and ensuring the free flow of information in the Asia Pacific region."[2] Four of the purposes of the framework are to[3]:

- develop appropriate privacy protections for personal information, particularly from the harmful consequences of unwanted intrusions and the misuse of personal information;
- enable global organizations that collect, access, use or process data in APEC Economies to develop and implement uniform approaches within their organizations for global access to and use of personal information;
- assist enforcement agencies in fulfilling their mandate to protect information privacy; and
- advance international mechanisms to promote and enforce information privacy and to maintain the continuity of information flows among APEC economies and with their trading partners.

4. In addition, the Privacy Framework calls for the development of a system of voluntary cross-border privacy rules for the APEC region in its "Guidance for International Implementation".[4]

5. These four purposes and the international implementation guidance formed the basis of the APEC Data Privacy Pathfinder, which was endorsed by APEC Ministers in September 2007 in Sydney, Australia. An APEC Pathfinder is a cooperative project among participating APEC Economies. The purpose of the Data Privacy Pathfinder was to develop a simple and transparent system that can be used by organizations for the protection of personal information that moves across APEC Economies. It was determined that the system should:

- provide a practical mechanism for participating Economies to implement the APEC Privacy Framework in an international, cross-border context; domestic laws, regulations and guidelines would continue to cover the collection and management of information within Economies;
- provide a means for organizations to transfer personal information across participating APEC Economies in a manner in which individuals may trust that the privacy of their personal information is protected; and

[1] Part IV of the Framework dealing with (a) guidance for domestic implementation and (b) guidance for international implementation was completed and endorsed by Ministers in 2005.
[2] APEC Privacy Framework, Part I, Preamble, para 4, 2005
[3] APEC Privacy Framework, Part I, Preamble, para 8, 2005
[4] APEC Privacy Framework, Part IV, Guidance on Int'l Implementation, Section III, paras 46-48.

- apply only to organizations (that is, businesses) – it is not intended to deal with the personal information handling practices of governments or individuals.

6. In the development of the APEC Data Privacy Pathfinder, the following stakeholder considerations were identified:

- organizations should have trust and confidence that organizations with which they enter into transactions that involve personal information have appropriate policies and procedures in place that are consistent with the APEC principles and respect applicable privacy and data security laws, as well as the privacy and security representations made to the individual when the personal information was collected;

- consumers should have trust and confidence that their personal information is transmitted and secured across borders; and

- governments should ensure that there are no unreasonable impediments to cross-border data transfers while at the same time protecting the privacy and security of their citizens' personal information domestically and, in cooperation with foreign governments, internationally.

7. The Pathfinder set out to develop a voluntary APEC Cross-Border Privacy Rules (CBPR) System, consistent with the above purposes, criteria and considerations, through the development of the following core documents:

- a detailed self-assessment questionnaire based on the nine APEC Privacy Principles for use by an applicant organization[5];

- a set of baseline program requirements based on the nine APEC Privacy Principles against which an APEC-recognized Accountability Agent will assess an organization's completed questionnaire[6];

- recognition criteria to be used by APEC Economies when considering the recognition of an Accountability Agent[7];

- the Cross Border Privacy Enforcement Arrangement[8] (CPEA); and

- the Charter of the Cross Border Privacy Rules Joint Oversight Panel[9] (JOP).

OPERATION OF THE CBPR SYTEM

Overview of the CBPR System

8. Organizations that choose to participate in the CBPR System should implement privacy policies and practices consistently with the CBPR program requirements for all personal information that they have collected or received that is subject to cross-border transfer to other participating

[5] See Project 1, CBPR Intake Questionnaire, 2011/SOM1/ECSG/DPS/020
[6] See Project 3, CBPR Program Requirements for use by Accountability Agents
[7] See Project 2, Accountability Agent Recognition Criteria, 2010/SOM1/ECSG/DPS/011
[8] See Projects 5/6/7, The Cross Border Privacy Enforcement Cooperation Arrangement, 2010/SOM1/ECSG/DPS/013
[9] See Charter of the Cross Border Privacy Rules Joint Oversight Panel, Annex A

APEC economies[10]. These privacy policies and practices should be evaluated by an APEC-recognized Accountability Agent for compliance with the CBPR program requirements. Once an organization has been certified for participation in the CBPR System, these privacy policies and practices will become binding as to that participant and will be enforceable by an appropriate authority, such as a regulator to ensure compliance with the CBPR program requirements.

Elements of the CBPR System

9. The CBPR System consists of four elements: (1) self-assessment; (2) compliance review; (3) recognition/acceptance; and (4) dispute resolution and enforcement.

CBPR ELEMENT 1 – SELF-ASSESSMENT

Self-Assessment Questionnaire for Organizations

10. The CBPR System relies on an organization's self-assessment of their data privacy policies and practices against the requirements of APEC Privacy Framework using an APEC-recognized CBPR questionnaire (*see para 21*). This questionnaire will be provided by the appropriate APEC-recognized Accountability Agent, in accordance with established selection requirements (*see para 38*).

Link to Compliance Review

11. The completed questionnaire and any associated documentation will then be submitted to the APEC-recognized Accountability Agent for confidential review against the baseline standards established in the CBPR program requirements (*see para 7*).

12. The submission of this questionnaire is the first step in an evaluative process that will determine whether an organization's privacy policies and practices are consistent with the program requirements of the CBPR System. This process can also be used by organizations to help them develop privacy policies or revise existing privacy policies to meet the program requirements of the CBPR System.

13. This questionnaire may be supplemented by additional questions, documentation or requests for clarification as part of the APEC-recognized Accountability Agent's review process.

Link to Compliance Directory

14. An organization that is found to be compliant with the CBPR program requirements by an APEC-recognized Accountability Agent will be certified as CBPR compliant and will have relevant details of their certification published in an APEC-hosted website so that consumers and other stakeholders can be made aware that the organization is an active participant in the CBPR System.

CBPR ELEMENT 2 – COMPLIANCE REVIEW

Accountability Agent Recognition Criteria

15. To become an APEC-recognized Accountability Agent, an Accountability Agent should meet the established recognition criteria to the satisfaction of APEC Economies (*see para 33*).

[10] While not required as part of the CBPR System, participating organizations are encouraged to apply the same privacy policies and procedures to all personal information that they have collected or received even if it is not subject to cross border transfer or if it is subject to such transfer only outside of participating APEC economies.

16. These criteria provide for the evaluation of an Accountability Agent's program requirements, dispute resolution procedures, and policies and procedures for the avoidance of conflicts of interest as well as process issues, including the certification and re-certification processes, ongoing monitoring and compliance reviews and enforcement of program requirements.

17. As a condition of APEC recognition, Accountability Agents are required to release anonymised case notes and complaint statistics. Complaint handling is an important element of the CBPR System. These actions will:

- promote understanding and increase transparency about the CBPR System;
- aid consistent interpretation of the APEC Privacy Principles and the CBPR System;
- provide additional guidance to organizations on the application of the APEC Privacy Principles and CBPR System; and
- promote accountability of those involved in complaints handling and build stakeholders' trust in the process.

18. As a further condition of APEC recognition, an Accountability Agent should consent to respond to requests from relevant government entities in any APEC Economy that reasonably relate both to that Economy and to the CBPR-related work of the Accountability Agent, where possible.

19. All APEC-recognized Accountability Agents should endeavour to cooperate when appropriate and where possible in CBPR-related complaint handling matters with other recognized Accountability Agents.

Compliance Review Process of CBPRs

20. When reviewing an organization's privacy policies and practices as described in the self-assessment questionnaire, an APEC-recognized Accountability Agent should assess them against the CBPR program requirements. These program requirements are designed to provide the minimum standard that applicant organizations should meet in order to ensure that the assessment process is conducted in a consistent manner across participating Economies. An APEC-recognized Accountability Agent's assessment process may exceed this standard but may not fall below it.

21. Where an applicant Accountability Agent intends to make use of its own questionnaire and/or program requirements in lieu of the APEC-recognized self-assessment questionnaire and/or the APEC-recognized CBPR program requirements (*see para 7*), it should establish its comparability to the satisfaction of APEC Economies as a condition of APEC recognition (*see para 54*).

CBPR ELEMENT 3 – RECOGNITION

Compliance Directory and Contact Information

22. APEC Economies will establish a publicly accessible directory of organizations that have been certified by Accountability Agents as compliant with the CBPR System. The directory will include contact point information that consumers can use to contact participating organizations. Each organization's listing will include the contact point information for the APEC-recognized Accountability Agent that certified the organization and the relevant Privacy Enforcement Authority. Contact point information allows consumers or other interested parties to direct questions and complaints to the appropriate contact point in an organization or to the relevant Accountability Agent, or if necessary, to contact the relevant Privacy Enforcement Authority.

23. The directory and contact lists will be hosted by the APEC Secretariat and maintained by the Electronic Commerce Steering Group in accordance with the APEC website Guidelines[11]. This website may be expanded to contain FAQs and additional information on the CBPR System for potential applicant organizations and for consumers.

CBPR ELEMENT 4 – ENFORCEMENT

Cooperation Arrangement for Cross-Border Privacy Enforcement

24. The CBPR system should be enforceable by Accountability Agents and Privacy Enforcement Authorities:

- Accountability Agents should be able to enforce the CBPR program requirements through law or contract; and
- The Privacy Enforcement Authorities should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the CBPR program requirements.

25. The CPEA, which was endorsed by APEC Ministers in November 2009 and commenced on 16 July 2010, aims to:

- facilitate information sharing among Privacy Enforcement Authorities (PE Authorities) in APEC Economies (which may include Privacy Commissioners' Offices, Data Protection Authorities or Consumer Protection Authorities that enforce Privacy Laws);
- provide mechanisms to promote effective cross-border cooperation between authorities in the enforcement of CBPR program requirements and privacy laws generally, including through referrals of matters and through parallel or joint investigations or enforcement actions; and
- encourage information sharing and cooperation on privacy investigation and enforcement with PE Authorities outside APEC (including by ensuring that the CPEA can work seamlessly with similar arrangements in other regions and at the global level).

26. The CPEA creates a framework for the voluntary sharing of information and provision of assistance for information privacy enforcement related activities. Any PE Authority in an APEC Economy may participate. Participating PE Authorities will contact each other for assistance or to make referrals regarding information privacy investigations and enforcement matters that involve each other's Economies. For example, during an investigation, a PE Authority in Economy X may seek the assistance of a PE Authority in Economy Y, if certain evidence of the alleged privacy violation (or the entity being investigated) is located in Economy Y. In that case, the PE Authority in Economy X may send a Request for Assistance to the point of contact in the PE Authority in Economy Y. The PE Authority in Economy Y may then consider the matter and provide assistance on a discretionary basis.

[11] http://webresources.apec.org/

CBPR PROCESS OVERVIEW

27. The following provides an overview of the process for participation by APEC Economies in the CBPR System, the process for the recognition of Accountability Agents by APEC Economies, the process for the certification of an organization, and the role Privacy Enforcement Authorities.

Process for Participation and Discontinuation of Participation by APEC Economies in the CBPR System

28. To participate in the CBPR System, an Economy must first satisfy the conditions in 2.2 of the Charter of the Joint Oversight Panel. The Economy then nominates one or more Accountability Agents for APEC recognition or notifies the ECSG Chair of receipt of application(s) for such recognition. Once at least one Accountability Agent has been recognised in relation to that Economy, organisations will be able to commence participation in the CBPR system in the Economy. Where only one Accountability Agent operates in an Economy and that Accountability Agent ceases to function in that capacity, the Economy's participation in the CBPR will be suspended upon a consensus determination by all other APEC Economies (excluding the Participating Economy in question) and the certification of those organizations certified by that Accountability Agent will be terminated until such time as the Economy is able to again fulfil the requirement for participation in the CBPR System, at which time any previously-certified applicant organizations should complete a new certification process.

29. An Economy may cease participation in the CBPR System at any time by giving one month's written notice to the APEC ECSG Chair. In the event that a Participant discontinues participation in the CBPR System, any APEC-recognized Accountability Agents in that Economy should terminate participation in the CBPR System in that Economy. This requirement should be incorporated into the agreements between the Accountability Agent and any organizations they certify as CBPR compliant.

Process for Recognition of Accountability Agents

30. An Economy can nominate an Accountability Agent operating within its jurisdiction for APEC recognition or, where appropriate, notify the Joint Oversight Panel that they have received a request for such recognition and submit the received application and associated documentation for consideration (*see para 54*). In either case, the Economy should describe the relevant domestic laws and regulations which may apply to the activities of Accountability Agents operating within their jurisdiction and the enforcement authority associated with these laws and regulations. Where the Privacy Enforcement Authority of an Economy assumes the role of Accountability Agent, the nomination may be done by the Economy with a confirmation that the Privacy Enforcement Authority is a participant of the CPEA as well as a summary of how that privacy enforcement authority may enforce the program requirements of the CBPR system.

31. In those instances where an Economy proposes to make use of an Accountability Agent in another participating APEC Economy to certify an applicant organization principally located within its borders, the proposing Economy should notify the Joint Oversight Panel of this proposal. The proposing Economy should describe to the Joint Oversight Panel the relevant domestic laws and regulations which may apply to the activities of Accountability Agents operating within their jurisdiction and the enforcement authority associated with these laws and regulations.

32. All applications for recognition will include a signed attestation by the Accountability Agent and all necessary supporting documentation as stipulated in the Accountability Agent recognition criteria.

33. Upon receipt of a request for recognition pursuant to paragraphs 30 or 31, the Joint Oversight Panel will commence a review of the required documentation and request any additional

information necessary to ensure the recognition criteria have been met. When the Joint Oversight Panel has completed this review process they will issue a recommendation to APEC Economies as to whether or not to recognize the Accountability Agent. Economies will consider the Accountability Agent's request for recognition, considering the recommendation of the Joint Oversight Panel. If no objections are received within a set deadline, the request will be considered to be approved by the ECSG.

34. Any APEC Economy has the right to reject the request of an Accountability Agent for such recognition.

35. The Joint Oversight Panel can receive complaints regarding the conduct of a recognized Accountability Agent by Economies, businesses, consumers or others at any time. Where appropriate, the Joint Oversight Panel can request the relevant Privacy Enforcement Authority or other relevant Authority in the Economy where the Accountability Agent is located to investigate the compliance of that Accountability Agent with their obligations established in the Recognition Criteria. The Privacy Enforcement Authority or other relevant Authority may investigate and take remedial action as necessary at its discretion as authorized under their domestic law. The Joint Oversight Panel may consider and recommend suspension of an Accountability Agent's recognition at any time.

36. APEC recognition will be limited to one year from the date of recognition, one month prior to which, an Accountability Agent should re-apply for APEC recognition, following the same process described above. During this time the Accountability Agent's recognition will continue.

37. When considering their recommendation to APEC Economies, the Joint Oversight Panel will consider any relevant information including complaints received regarding the conduct of a recognized Accountability Agent by Economies, businesses, consumers or others in the previous year as well as any investigation request by the Joint Oversight Panel to Privacy Enforcement Authorities or other relevant Authorities.

Process for Certification of Organizations

38. Applicant organizations should make use of Accountability Agents located within the jurisdiction in which the applicant organization is primarily located or an Accountability Agent recognized pursuant to paragraph 31.

39. Once an applicant organization selects and contacts an eligible APEC-recognized Accountability Agent, the Accountability Agent will provide the self-assessment questionnaire to the organization for completion and will review the answers and any supporting documentation based on its assessment guidelines or make use of APEC-recognized documentation and review procedures.

40. The proposed application process would be iterative and allow for back and forth discussions between the applicant organization and the Accountability Agent.

41. The Accountability Agent Recognition Criteria describe the role of Accountability Agents as follows:

- The Accountability Agent is responsible for the self-assessment and compliance review phases of the CBPR System accreditation process. Applicant organizations will be responsible for developing their privacy policies and practices and may only participate in the CBPR System if these policies and practices are certified by the relevant Accountability Agent to be compliant with the requirements of the CBPR System. It is the responsibility of the Accountability Agent to certify an organization's compliance with these requirements.

- The self-assessment questionnaire and assessment guidelines are publicly-available documents and prospective applicant organizations will have access to the guidelines so that they can see how their responses to the self-assessment questionnaire will be assessed. In considering how best to assist prospective applicant organizations, a recognized Accountability Agent may wish to develop additional documentation outlining their review process.

Role of the Privacy Enforcement Authority

42. The CPEA defines'Privacy Enforcement Authority' as any public body that is responsible for enforcing Privacy Law, and that has powers to conduct investigations or pursue enforcement proceedings. 'Privacy Law' is then defined as laws and regulations of an APEC Economy, the enforcement of which have the effect of protecting personal information consistent with the APEC Privacy Framework.

- The Privacy Enforcement Authority must be able to review a CBPR complaint/issue if it cannot be resolved by the participating organization in the first instance or by the Accountability Agent and when appropriate, investigate and take enforcement action. The Privacy Enforcement Authority has the discretion to decide whether or not to deal with a Request for Assistance made by another Privacy Enforcement Authority.

- CPEA participation is the predicate step to any Economies' involvement in the CBPR System as the CPEA establishes that the Economy has a law in place "the enforcement of which, has the effect of implementing the APEC Privacy Framework."

THE CBPR SYSTEM AND DOMESTIC LAWS AND REGULATIONS

43. The CBPR System does not displace or change an Economy's domestic laws and regulations. Where there are no applicable domestic privacy protection requirements in an Economy, the CBPR System is intended to provide a minimum level of protection.

44. Participation in the CBPR System does not replace a participating organization's domestic legal obligations. The commitments which an organization carries out in order to participate in the CBPR System are separate from any domestic legal requirements that may be applicable. Where domestic legal requirements exceed what is expected in the CBPR System, the full extent of such domestic law and regulation will continue to apply. Where requirements of the CBPR System exceed the requirements of domestic law and regulation, an organization will need to voluntarily carry out such additional requirements in order to participate. Nonetheless, Privacy Enforcement Authorities in that Economy should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the CBPR program requirements.

45. For the purposes of participation in the CBPR System, an Accountability Agent's verification will only apply to an organization's compliance with its CBPR commitments, not its compliance with applicable domestic legal requirements.

46. Where an Economy's domestic laws and regulations preclude or restrict that Economy's ability to participate in the CBPR System, it is a matter for the Economy to consider whether and how to modify the applicable domestic laws to facilitate participation.

47. It is not the purpose of the CBPR System to direct Economies on whether and how to modify domestic laws and regulations. This is a matter to be addressed through capacity building activities and other guidance run through the Data Privacy Sub-Group.

48. However, when considering whether to participate in the CBPR System, Economies may need to make changes to domestic laws and regulations to ensure the necessary elements of the CBPR System are in place – for example, Economies are to identify an appropriate regulatory authority as defined in the Cross Border Privacy Enforcement Arrangement (CPEA) to act as the privacy enforcement authority in the CBPR System.

GOVERNANCE OF THE CBPR SYSTEM

Objective

49. The CBPR System requires governance mechanisms that will perform essential operations in the administration and maintenance of the System. In the development of the governance model, a number of basic principles were identified:

- Simplicity;
- Transparency;
- Low cost; and
- Accountability to APEC Economies.

50. As the APEC representative body established to deal with data privacy issues, the Data Privacy Sub-Group is responsible for the governance of the CBPR System. Governance mechanisms should enable the day-to-day running of the CBPR System without the continuous involvement of the Sub-Group, which only meets twice a year.

51. As APEC is a non-treaty organization with a small full-time staff, governance of the CBPR System cannot impose onerous duties on either the Secretariat or Economies.

Functions of the Governance Model

52. Regardless of these limitations, the governance model should nonetheless deal with the essential administrative functions required for the CBPR System to effectively operate. These essential functions include:

- Developing and maintaining a staffing and revenue structure to support the CBPR System;
- Managing the APEC-hosted compliance directory (*see para 14*);
- Facilitating participation in the CBPR System by APEC Economies, including through capacity-building activities;
- Assessing and monitoring the compliance of recognized Accountability Agents against the Recognition Criteria;
- Managing the Cross Border Privacy Enforcement Arrangement and associated documents and procedures; and

- Developing education materials to facilitate a region-wide understanding of the elements of the CBPR System and its program requirements.

Joint Oversight Panel

53. In recognition of these requirements, Economies are to establish a Joint Oversight Panel made up of nominated Economies approved by, and operating on behalf of, the Data Privacy Sub-Group. This model provides a clear line of authority for the operation of the CBPR System from the ECSG through the Data Privacy Sub-Group, in which all APEC Economies can participate.

54. The core functions of the Joint Oversight Panel are set out in 6.2 of *Charter of the APEC Cross-Border Privacy Rules System Joint Oversight Panel* (Annex A)

55. To assist the Joint Oversight Panel with the identified core functions, working groups on certification and enforcement should be established. The working groups are to provide representative oversight and leadership for the certification, operations, and enforcement of the CBPR System. The Joint Oversight Panel may establish more working groups as needed.

56. In addition to the foregoing, it is necessary to establish a process through which the Data Privacy Sub-Group can monitor, evaluate and review the entirety of the CBPR System. This process should allow Economies to develop and revise the CBPR System in response to practical experience and the changing needs of Economies.

SUCCESS CRITERIA FOR THE CBPR SYSTEM

57. The CBPR System implements the Data Privacy Pathfinder. The CBPR System should recognise and incorporate the core APEC principles of voluntarism, comprehensiveness, consensus-based decision making, flexibility, transparency, open regionalism and differentiated implementation timetables for developed and developing Economies.

58. In recognition of these core APEC principles, the CBPR System should satisfy the objectives set out in the Data Privacy Pathfinder:

- promote a conceptual framework of principles of how cross-border privacy rules should work across APEC Economies;
- develop and support consultative processes between regulators, responsible agencies, lawmaking bodies, industry, third party solution providers, consumer and privacy representatives;
- produce practical documents and procedures that underpin cross-border privacy rules;
- explore ways in which various documents and procedures can be implemented in practice; and
- promote education and outreach on how an accountable CBPR System works.

59. There are three key specific criterion for judging success of both the individual projects and the Pathfinder as a whole:

- the effective protection of consumer personal information privacy in a system trusted by consumers;

- that implementation can be flexible enough to be adapted to the particular domestic legal environment of APEC Economies, while providing certainty for system participants; and
- the regulatory burden on business is minimised while allowing business to develop and comply with effective and coherent rules for cross-border flows of personal information.

ANNEX A

CHARTER OF THE APEC CROSS-BORDER PRIVACY RULES SYSTEM JOINT OVERSIGHT PANEL

1. CHARACTER OF THIS DOCUMENT

1.1 This Charter is to be read consistently with the APEC Privacy Framework. Nothing in this Charter is intended to:

i. Create any binding obligations on APEC Economies and/or their government agencies, or affect their existing rights and obligations under international or domestic law;
ii. Impede any governmental activities authorized by domestic or international law;
iii. Create any obligations or expectations of cooperation that would exceed a CBPR Participant's scope of authority and jurisdiction; or
iv. Create obligations or expectations for non-participating government agencies.

2. COMMENCEMENT OF PARTICIPATION IN THE CROSS BORDER PRIVACY RULES SYSTEM

2.1 This Charter will take effect upon endorsement by the Electronic Commerce Steering Group (ECSG).

2.2 An APEC Member Economy is considered a Participant in the Cross Border Privacy Rules (CBPR) System (CBPR Participant), after the Chair of the Electronic Commerce Steering Group (ECSG Chair) has notified the Economy that the following conditions have been met:

(i) The Economy's ECSG delegation, or appropriate governmental representative, submits to the ECSG Chair a letter indicating its intention to participate and confirming that at least one Privacy Enforcement Authority in that Economy is a participant in the APEC Cross Border Privacy Enforcement Arrangement (CPEA);

(ii) The Economy indicates its intention to make use of at least one APEC-recognized Accountability Agent subject to the procedures outlined in paragraph 6.2;

(iii) The Economy's ECSG delegation, or appropriate governmental representative, after consulting with the Joint Oversight Panel, submits to the Chair of the ECSG an explanation of how the CBPR System program requirements may be enforced in that Economy; and

(iv) The Joint Oversight Panel submits to the Chair of the ECSG a report as to how the conditions in (i)-(iii) above have been satisfied.

3. TRANSPARENCY

3.1 A CBPR Participant will provide notice to the APEC ECSG Chair of any new laws or regulations and any amendments to existing laws or regulations as well as all other developments that may affect the operation and enforcement of the CBPR System.

3.2 The APEC ECSG Chair will promptly notify APEC Economies of any notification received pursuant to paragraph 3.1.

4. TERMINATION OF PARTICIPATION

4.1 A CBPR Participant may cease participation in the CBPR System by giving one month's written notice to the APEC ECSG Chair.

4.2 The APEC ECSG Chair will promptly notify APEC Economies of any notification received pursuant to paragraph 4.1.

4.3 In the event that a CBPR Participant terminates participation in the CBPR System, or is suspended or terminated from the CBPR System, recognition of any previously recognized Accountability Agent to operate in that Participant's Economy will automatically suspend or terminate and the certification of those organizations certified by that Accountability Agent will be terminated until such time as the Economy is able to again fulfil the requirement for participation in the CBPR System, at which time any previously-certified applicant organizations should complete a new certification process.

5. CAUSE FOR SUSPENSION OR TERMINATION

5.1 Participation by an APEC Economy in the CBPR System may be suspended or terminated by a consensus determination by the other APEC Economies that one or more of the following conditions have been met:

i. Revocation, repeal or amendment of any domestic laws and/or regulations having the effect of making participation in the APEC CBPR System impossible;
ii. The CBPR Participant's Privacy Enforcement Authority as defined in paragraph 4.1 of the CPEA ceases participation pursuant to paragraph 8.2 of the CPEA; or
iii. Dissolution or disqualification of a previously recognized Accountability Agent where this function is provided exclusively in the CBPR Participant's Economy by that entity.

5.2 A request for a consensus determination that any condition identified in paragraph 5.1 has been met may be made by any CBPR Participant at any time.

6. JOINT OVERSIGHT PANEL

6.1 The ECSG hereby establishes a Joint Oversight Panel, consisting of representatives from three APEC Economies, for a two-year appointment, subject to ECSG endorsement and the terms set out in paragraph 7.2. The ECSG will endorse a Chairperson for a two-year appointment from these three Economies. The Joint Oversight Panel will meet at the request of the ECSG, or more frequently as decided by CBPR Participants to assist in the effective implementation of the CBPR System. The ECSG may appoint succeeding panels as it may deem appropriate.

6.2 The Joint Oversight Panel will perform the following functions:

i. Engage in consultations with those Economies that have indicated an intention to participate in the CBPR System and issue a report as to how the conditions set out in paragraph 2.2 have been met;
ii. Make recommendations to the APEC Economies whether to recognize an applicant Accountability Agent as compliant with the requirements of the CBPR System. In making such recommendations, the Joint Oversight Panel should be satisfied of the following:

a) The applicant Accountability Agent has a location in a CBPR Participant's Economy or is subject to the jurisdiction of the relevant privacy enforcement authority in that Economy, and
b) The applicant Accountability Agent meets the Recognition Criteria established under the CBPR System and has provided all necessary documentation as requested by the Joint Oversight Panel;

iii. Consider and recommend suspension of the recognition of an Accountability Agent at any time;
iv. Collect all case notes received by recognized Accountability Agents as required under the Accountability Agent Recognition Criteria and circulate to APEC Economies;
v. Collect complaint statistics from recognized Accountability Agents as required under the Accountability Agent Recognition Criteria and circulate to APEC Economies;
vi. Advise recognized Accountability Agents whether or not to withdraw from particular engagements if a potential conflict is alleged, considering any evidence provided by the recognized Accountability Agents as to internal structure and procedural safeguards that are in place to address any potential and actual conflicts of interest;
vii. Verify that each recognized Accountability Agent complies with the re-certification process as required under the Accountability Agent Recognition Criteria;
viii. Review any reported material change by the recognized Accountability Agent (e.g. ownership, structure or policies) as required under the Accountability Agent Recognition Criteria and report to APEC Economies its recommendation as to whether such change impacts the appropriateness of recognizing the Accountability Agent as compliant with the requirements of the CBPR System;
ix. Facilitate the review and edit of primary documentation associated with the CBPR System when necessary in conjunction with APEC Economies; and
x. Perform all other functions as identified and decided by APEC Economies as necessary to the operation of the CBPR System.

6.3 All recommendations of the Joint Oversight Panel will be made by simple majority. A dissenting member of the Joint Oversight Panel may circulate its dissent from the majority's recommendation on any matter to APEC Economies.

6.4 In no circumstance should a member of the Joint Oversight Panel participate in any of the activities under 6.2 when the Accountability Agent is a public (or governmental) entity in the member's Economy or any of the activities under 2.2 where the interested Economy is a member of the Joint Oversight Panel. In such instances, the Data Privacy Subgroup Chair will designate another APEC Economy to temporarily function as a member of the Joint Oversight Panel.

6.5 The Joint Oversight Panel may establish working teams to address each of the above functions and request assistance from the APEC Secretariat or APEC Economies as necessary.

6.6 Recommendations by the Joint Oversight Panel will take effect upon endorsement by the ECSG.

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.