Guidebook on APEC privacy and trustmark

Prepared or Printed by:
Vietnam E-commerce Develoment Center
Minitry of Industry and Trade, Vietnam
Add: 25 Ngo Quyen Str., Hoan Kiem Distrist, Hanoi, Vietnam
Phone: 84-4-22205363 / Fax: 84-4-22205507
Website: http://ecomviet.vn
APEC Publication Number: APEC#212-CT-03.2
ISBN: 978-981-07-4079-5

Produced for:
Asia-Pacific Economic Cooporation Secretariat
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6891-9600 Fax: (65) 6891-9690
Email: info@apec.org Website: www.apec.org

Guidebook on APEC privacy and trustmark

Asia-Pacific
Economic Cooperation

Guidebook on APEC privacy and trustmark

E-commerce Steering Group

APEC privacy and trustmark

1. APEC economies recognize the importance of protecting information privacy and maintaining information flows among economies in the Asia Pacific region and among their trading partners. As APEC Ministers acknowledged in endorsing the 1998 Blueprint for Action on Electronic Commerce, the potential of electronic commerce cannot be realized without government and business cooperation "to develop and implement technologies and policies, which build trust and confidence in safe, secure and reliable communication, information and delivery systems, and which address issues including privacy...". The lack of consumer trust and confidence in the privacy and security of online transactions and information networks is one element that may prevent member economies from gaining all of the benefits of electronic commerce. APEC economies realize that a key part of efforts to improve consumer confidence and ensure the growth of electronic commerce must be cooperation to balance and promote both effective information privacy protection and the free flow of information in the Asia Pacific region.

2. Information and communications technologies, including mobile technologies, that link to the Internet and other information networks have made it possible to collect, store and access information from anywhere in the world. These technologies offer great potential for social and economic benefits for business, individuals and governments, including increased consumer choice, market expansion, productivity, education and product innovation. However, while these technologies make it easier and cheaper to collect, link and use large quantities of information, they also often make these activities undetectable to individuals. Consequently, it can be more difficult for individuals to retain a measure of control over their personal information. As a result, individuals have become concerned about the harmful consequences that may arise from the misuse of their information. Therefore, there is a need to promote and enforce ethical and trustworthy information practices in on- and off-line contexts to bolster the confidence of individuals and businesses.

3. As both business operations and consumer expectations continue to shift due to changes in technology and the nature of information flows, businesses and other organizations require simultaneous input and access to data 24-hours a day in order to meet customer and societal needs, and to provide efficient and cost-effective services. Regulatory systems that unnecessarily restrict this flow or place burdens on it have adverse implications for global business and economies. Therefore, in promoting and enforcing ethical information practices, there is also a need to develop systems for protecting information privacy that account for these new realities in the global environment.

4. APEC economies endorse the principles-based APEC Privacy 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.

5. This Framework, which aims at promoting electronic commerce throughout the Asia Pacific region, is consistent with the core values of the OECD's 1980 Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (OECD Guidelines)1, and reaffirms the value of privacy to individuals and to the information society.

6. The Framework specifically addresses these foundation concepts, as well as issues of particular relevance to APEC member economies. Its distinctive approach is to focus attention on practical and consistent information privacy protection within this context. In so doing, it balances

information privacy with business needs and commercial interests, and at the same time, accords due recognition to cultural and other diversities that exist within member economies.

7. The Framework is intended to provide clear guidance and direction to businesses in APEC economies on common privacy issues and the impact of privacy issues upon the way legitimate businesses are conducted. It does so by highlighting the reasonable expectations of the modern consumer that businesses will recognize their privacy interests in a way that is consistent with the Principles outlined in this Framework.

8. Finally, this Framework on information privacy protection was developed in recognition of the importance of:

• Developing appropriate privacy protections for personal information, particularly from the harmful consequences of unwanted intrusions and the misuse of personal information;

• Recognizing the free flow of information as being essential for both developed and developing market economies to sustain economic and social growth;

• Enabling global organizations that collect, access, use or process data in APEC member economies to develop and implement uniform approaches within their organizations for global access to and use of personal information;

• Enabling enforcement agencies to fulfill their mandate to protect information privacy; and,

• Advancing international mechanisms to promote and enforce information privacy and to maintain the continuity of information flows among APEC economies and with their trading partners.

Asia-Pacific Economic Cooperation

Part II. Scope

The purpose of Part II of the APEC Privacy Framework is to make clear the extent of coverage of the Principles.

9. Personal information means any information about an identified or identifiable individual.

The Principles have been drafted against a background in which some economies have well-established privacy laws and/or practices while others may be considering the issues. Of those with already settled policies, not all treat personal information in exactly the same way. Some, for example, may draw distinctions between information that is readily searchable and other information. Despite these differences, this Framework has been drafted to promote a consistent approach among the information privacy regimes of APEC economies.

This Framework is intended to apply to information about natural living persons, not legal persons. The APEC Privacy Framework applies to personal information, which is information that can be used to identify an individual.

It also includes information that would not meet this criteria alone, but when put together with other information would identify an individual, individual's personal, family or household affairs.

10. Personal information controller means a person or organization who controls the

10. The APEC Privacy Framework applies to persons or organizations in the public and private sectors who control

collection, holding, processing or use of personal information. It includes a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf, but excludes a person or organization who performs such functions as instructed by another person or organization. It also excludes an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.	the collection, holding, processing, use, transfer or disclosure of personal information. Individual economies' definitions of personal information controller may vary. However, APEC economies agree that for the purposes of this Framework, where a person or organization instructs another person or organization to collect, hold, use, process, transfer or disclose personal information on its behalf, the instructing person or organization is the personal information controller and is responsible for ensuring compliance with the Principles. Individuals will often collect, hold and use personal information for personal, family or household purposes. For example, they often keep address books and phone lists or prepare family newsletters. The Framework is not intended to apply to such personal, family or household activities.
11. Publicly available information means personal information about an individual that the individual knowingly makes or permits to be made available to the public, or is legally obtained and accessed from: a) government records that are available to the public; b) journalistic reports; or c) information required by law to be made available to the public.	The APEC Privacy Framework has limited application to publicly available information. Notice and choice requirements, in particular, often are superfluous where the information is already publicly available, and the personal information controller does not collect the information directly from the individual concerned. Publicly available information may be contained in government records that are available to the public, such as registers of people who are entitled to vote, or in news items broadcast or published by the news media.

12. In view of the differences in social, cultural, economic and legal backgrounds of each member economy, there should be flexibility in implementing these Principles.	Although it is not essential for electronic commerce that all laws and practices within APEC be identical in all respects, including the coverage of personal information, compatible approaches to information privacy protection among APEC economies will greatly facilitate international commerce. These Principles recognize that fact, but also take into account social, cultural and other differences among economies. They focus on those aspects of privacy protection that are of the most importance to international commerce.
13. Exceptions to these Principles contained in Part III of this Framework, including those relating to national sovereignty, national security, public safety and public policy should be: **a) limited and proportional to meeting the objectives to which the exceptions relate; and,** **b) (i) made known to the public; or,** **(ii)in accordance with law.**	The Principles contained in Part III of the APEC Privacy Framework should be interpreted as a whole rather than individually, as there is a close relationship among them. For example, the Use Principle is closely related to both the Notice and Choice Principles. Economies implementing the Framework at a domestic level may adopt suitable exceptions that suit their particular domestic circumstances. Although recognizing the importance of governmental respect for privacy, this Framework is not intended to impede governmental activities authorized by law when taken to protect national security, public safety, national sovereignty or other public policy. Nonetheless, Economies should take into consideration the impact of these activities upon the rights, responsibilities and legitimate interests of individuals and organizations.

Part III. APEC information Privacy priciples

I. Preventing Harm

14. Recognizing the interest of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.

The Preventing Harm Principle recognizes that one of the primary objectives of the APEC Privacy Framework is to prevent misuse of personal information and consequent harm to individuals. Therefore, privacy protection, including self –regulatory efforts, education and awareness campaigns, laws, regulations and enforcement mechanism, should be designed to prevent harm to individuals from the wrongful collection and misuse of their personal information. Hence, remedies for privacy infringements should be designed to prevent harms resulting from the wrongful collection of misuse of personal information, and should be proportionate to the likelihood and severity of any harm threatened by the collection or use of personal information.

II. Notice

15. Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include:

The Notice Principle is directed towards ensuring that individuals are able to know what information is collected about them and for what purpose it is to be used. By providing notice, personal information controllers may enable an individual to make a more informed decision about interacting with the organization. One common method of compliance with this Principle is for personal information

a) the fact that personal information is being collected;

b) the purposes for which personal information is collected;

c) the types of persons or organization to whom personal information might be disclosed;

d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information;

e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.

controllers to post notices on their Web sites. In other situations, placement of notices on intranet sites or in employee handbooks, for example, may be appropriate.

The requirement in this Principle relating to when notice should be provided is based on a consensus among APEC member economies. APEC member economies agree that good privacy practice is to inform relevant individuals at the time of, or before, information is collected about them. At the same time, the Principle also recognizes that there are circumstances in which it would not be practicable to give notice at or before the time of collection, such as in some cases where electronic technology automatically collects information when a prospective customer initiates contact, as is often the case with the use of cookies.

Moreover, where personal information is not obtained directly from the individual, but from a third party, it may not be practicable to give notice at or before the time of collection of the information. For example, when an insurance company collects employees' information from an employer in order to provide medical insurance services, it may not be practicable for the insurance company to give notice at or before the time of collection of the employees' personal information.

16. All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice should be provided as soon after as is practicable.

17. It may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information.

Additionally, there are situations in which it would not be necessary to provide notice, such as in the collection and use of publicly available information, or of business contact information and other professional information that identifies an individual in his or her professional capacity in a business context. For example, 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.

Further, if colleagues who work for the same company as the individual, were to provide the individual's business contact information to potential customers of that company, the individual would not have an expectation that notice would be provided regarding the transfer or the expected use of that information.

III. Collection Limitation

18. The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.

This Principle limits collection of information by reference to the purposes for which it is collected. The collection of the information should be relevant to such purposes, and proportionality to the fulfillment of such purposes may be a factor in determining what is relevant.

This Principle also provides that collection methods must be lawful and fair. So, for example, obtaining personal

information under false pretenses (e.g., where an organization uses telemarketing calls, print advertising, or email to fraudulently misrepresent itself as another company in order to deceive consumers and induce them to disclose their credit card numbers, bank account information or other sensitive personal information) may in many economies be considered unlawful. There fore, even in those economies where there is no explicit law against these specific methods, they may be considered an unfair means of collection.

The Principle also recognizes that there are circumstances where providing notice to, or obtaining consent of, individuals would be inappropriate. For example, in a situation where there is an outbreak of food poisoning, it would be appropriate for the relevant health authorities to collect the personal information of patrons from restaurants without providing notice to or obtaining the consent of individuals in order to tell them about the potential health risk.

IV. Uses of Personal Information

19. Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except:

The Use Principle limits the use of personal information to fulfilling the purposes of collection and other compatible or related purposes. For the purposes of this Principle, "uses of personal information" includes the transfer or 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.

a) with the consent of the individual whose personal information is collected;
b) when necessary to provide a service or product requested by the individual; or,
c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.

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" would 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.

V. Choice

20. Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.

The general purpose of the Choice Principle is to ensure that individuals are provided with choice in relation to collection, use, transfer and disclosure of their personal information. Whether the choice is conveyed electronically, in writing or by other means, notice of such choice should be clearly worded and displayed clearly and conspicuously. By the same token, the mechanisms for exercising choice should be accessible and affordable to individuals. Ease of access and convenience are factors that should be taken into account.

Where an organization provides information on available mechanisms for exercising choice that is specifically tailored to individuals in an APEC member economy or national group, this may

require that the information be conveyed in an "easily understandable" or particular way appropriate to members of that group (e.g., in a particular language). However if the communication is not directed to any particular economy or national group other than the one where the organization is located, this requirement will not apply.

This Principle also recognizes, through the introductory words "where appropriate", 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. As is specified in the Principle, APEC member economies agree that in many situations it would not be necessary or practicable to provide a mechanism to exercise choice when collecting publicly available information. For example, it would not be necessary to provide a mechanism to exercise choice to individuals when collecting their name and address from a public record or a newspaper.

In addition to situations involving publicly available information, APEC member economies also agreed that in specific and limited circumstances it would not be necessary or practicable to provide a mechanism to exercise choice when collecting, using, transferring or disclosing other types of information. For example, when business contact information or other professional information that identifies an individual in his or her professional capacity is being exchanged in a business context it is generally impractical or unnecessary to provide amechanism to exercise choice, as in these circumstances individuals would expect that their information be used in this way.

Further, in certain situations, it would not be practicable for employers to be subject to requirements to provide a mechanism to exercise choice related to the personal information of their employees when using such information for employment purposes. For example, if an organization has decided to centralize human resources information, that organization should not be required to provide a mechanism to exercise choice to its employees before engaging in such an activity.

VI. Integrity of Personal Information

21. Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.

This Principle recognizes that a personal information controller is obliged to maintain the accuracy and completeness of records and keep them up to date. Making decisions about individuals based on inaccurate, incomplete or out of date information may not be in the interests of individuals or organizations. This Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use.

VII. Security Safeguards

22. Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized

This Principle recognizes that individuals who entrust their information to another are entitled to expect that their information be protected with reasonable security safeguards.

destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.

VIII. Access and Correction

23. Individuals should be able to:

a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them;

b) have communicated to them, after having provided sufficient proof of their identity, personal information about them;

i. within a reasonable time;

ii. at a charge, if any, that is not excessive;

iii. in a reasonable manner;

iv. in a form that is generally understandable; and,

c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.

The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right. This Principle includes specific conditions for what would be considered reasonable in the provision of access, including conditions related to timing, fees, and the manner and form in which access would be provided. What is to be considered reasonable in each of these areas will vary from one situation to another depending on circumstances, such as the nature of the information processing activity. Access will also be conditioned bysecurity requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision oaccess.

Access must be providedina reasonable manner and form. A reasonable manner should include the normal methods of interaction between orga nizations and individuals. For example, if a computer was involved in the transaction or request, and the individual's

24. Such access and opportunity for correction should be provided except where:

(i) 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;

(ii) the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or

(iii) the information privacy of persons other than the individual would be violated.

25. If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial.

email address is available, email would be considered "a reasonable manner" to provide information. Organizations that have transacted with an individual may reasonably be expected to answer requests in a form that is similar to what has been used in prior exchanges with said individual or in the form that is used and available within the organization, but should not be understood to require separate language translation or conversion of code into text.

Both the copy of personal information supplied by an organization in response to an access request and any explanation of codes used by the organization should be readily comprehensible. This obligation does not extend to the conversion of computer language (e.g. machine-readable instructions, source codes or object codes) into text. However, where a code represents a particular meaning, the personal information controller shall explain the meaning of that code to the individual. For example, if the personal information held by the organization includes the age range of the individual, and that is represented by a particular code (e.g., "1" means 18-25 years old, "2" means "26-35 years old, etc.), then when providing the individual with such a code, the organization shall explain to the individual what age range that code represents.

Where individual requests access to his or her information, that information should be provided in the language in which it is currently held. Where information is held in a language different

to the language of original collection, and if the individual requests the information be provided in that original language, an organization should supply the information in the original language if the individual pays the cost of translation.

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.

Consistent with the fundamental nature of access, organizations should always make good faith efforts to provide access. For example, where certain information needs to be protected and can be readily separated from other information subject to an access request, the organization should redact the protected information and make available the other information. However, in some situations, it may be necessary for organizations to deny claims for access and correction, and this Principle sets out the conditions that must be met in order for such denials to be considered acceptable, which include: situations where claims would constitute an unreasonable expense or burden on the personal information controller, such as when claims for access are repetitious or vexatious by nature; cases where providing the information would constitute a violation of laws or would compromise security; or, incidences where it would be necessary in order to protect commercial confidential has taken steps

information that an organization to protect from disclosure, where disclosure would benefit a competitor in the marketplace, such as a particular computer or modeling program.

"Confidential commercial information" is information that an organization has taken steps to protect from disclosure, where such disclosure would facilitate a competitor in the market to use or exploit the information against the business interest of the organization causing significant financial loss. The particular computer program or business process an organization uses, such as a modeling program, or the details of that program or business process may be confidential commercial information. Where confidential commercial information can be readily separated from other information subject to an access request, the organization should redact the confidential commercial information and make available the non-confidential information, to the extent that such information constitutes personal information of the individual concerned. Organizations may deny or limit access to the extent that it is not practicable tseparate the personal information from the confidential commercial information and where granting access would reveal the organization's own confidential commercial information as defined above, or where it would reveal the confidential commercial information of another organization that is subject to an obligation of confidentiality.

When an organization denies a request for access, for the reasons specified above, such an organization should provide the individual with anexplanation as to why it has made that determination and information on how to challenge that denial. An organization would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order.

IX. Accountability

26. A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.

Efficient and cost effective business models often require information transfers between different types of organizations in different locations with varying relationships. When transferring information, personal information controllers should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, information controllers should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between the personal information controller and the third party to whom the information is disclosed. In these types of circumstances, personal information controllers 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, the personal information controller would be relieved of any due diligence or consent obligations.

Part IV. Implementation

27. Part IV provides guidance to Member Economies on implementing the APEC Privacy Framework. Section A focuses on those measures Member Economies should consider in implementing the Framework domestically, while Section B sets out APEC-wide arrangements for the implementation of the Framework's cross-border elements.

A. GUIDANCE FOR DOMESTIC IMPLEMENTATION

I. Maximizing Benefits of Privacy Protections and Information Flows

28. Economies should have regard to the following basic concept in considering the adoption of measures designed for domestic implementation of the APEC Privacy Framework:

29. Recognizing the interests of economies in maximizing the economic and social benefits available to their citizens and businesses, personal information should be collected, held, processed, used, transferred, and disclosed in a manner that protects individual information privacy and allows them to realize the benefits of information flows within and across borders.

30. Consequently, as part of establishing or reviewing their privacy protections, Member Economies, consistent with the APEC Privacy Framework and any existing domestic privacy protections, should take all reasonable and appropriate steps to identify and remove unnecessary barriers to information flows and avoid the creation of any such barriers.

II. Giving Effect to the APEC Privacy Framework

31. There are several options for giving effect to the Framework and securing privacy protections for individuals including legislative, administrative,

industry self- regulatory or a combination of these methods under which rights can be exercised under the Framework. In addition, Member Economies should consider taking steps to establish access point(s) or mechanisms to provide information generally about the privacy protections within its jurisdiction. In practice, the Framework is meant to be implemented in a flexible manner that can accommodate various methods of implementation, including through central authorities, multi-agency enforcement bodies, a network of designated industry bodies, or a combination of the above, as Member Economies deem appropriate.

32. As set forth in Paragraph 31, the means of giving effect to the Framework may differ between Member Economies, and it may be appropriate for individual economies to determine that different APEC Privacy Principles may call for different means of implementation. Whatever approach is adopted in a particular circumstance, the overall goal should be to develop compatibility of approaches in privacy protections in the APEC region that is respectful of requirements of individual economies.

33. APEC economies are encouraged to adopt non-discriminatory practices in protecting individuals from privacy protection violations occurring in that Member Economy's jurisdiction.

34. Discussions with domestic law enforcement, security, public health, and other agencies are important to identify ways to strengthen privacy without creating obstacles to national security, public safety, and other public policy missions.

III. Educating and publicising domestic privacy protections

35. For all Member Economies, in particular those Member Economies in earlier stages of development of their domestic approaches to privacy protections, the Framework is intended to provide guidance in developing their approaches.

36. For the Framework to be of practical effect, it must be known and accessible. Accordingly, Member Economies should:

a) publicise the privacy protections it provides to individuals;

b) educate personal information controllers about the Member Economy's privacy protections; and,

c) educate individuals about how they can report violations and how remedies can be pursued.

IV. Cooperation between the Public and Private Sectors

37. Active participation of non-governmental entities will help ensure that the full benefits of the APEC Privacy Framework can be realized. Accordingly, Member Economies should engage in a dialogue with relevant private sector groups, including privacy groups and those representing consumers and industry, to obtain input on privacy protection issues and cooperation in furthering the Framework's objectives. Furthermore, especially in the economies where they have not established privacy protection regimes in their domestic jurisdiction, Member Economies should pay ample attention to whether private sector's opinions are reflected in developing privacy protections. In particular, Member Economies should seek the cooperation of non-governmental entities in public education and encourage their referral of complaints to privacy enforcement agencies, as well as their continuing cooperation in the investigation of those complaints.

V. Providing for appropriate remedies in situations where privacy protections are violated

38. A Member Economy's system of privacy protections should include an appropriate array of remedies for privacy protection violations, which could include redress, the ability to stop a violation from continuing, and other remedies. In determining the range of remedies for privacy protection violations, a number of factors should be taken into account by a Member Economy including:

a) the particular system in that Member Economy for providing privacy protections (e.g., legislative enforcement powers, which may include rights of individuals to pursue legal action, industry self-regulation, or combination of systems); and

b) the importance of having a range of remedies commensurate with the extent of the actual or potential harm to individuals resulting from such violations.

VI. Mechanism for Reporting Domestic Implementation of the APEC Privacy Framework

39. Member economies should make known to APEC domestic implementation of theFramework through the completion of and periodic updates to the Individual Action Plan (IAP) on Information Privacy.

B. GUIDANCE FOR INTERNATIONAL IMPLEMENTATION

In addressing the international implementation of the APEC Privacy Framework, and consistent with the provisions of Part A, Member Economies should consider the following points relating to the protection of the privacy of personal information:

I. Information sharing among Member Economies

40. Member Economies are encouraged to share and exchange information, surveys and research in respect of matters that have a significant impact on privacy protection.

41. In furthering the objectives of paragraphs 35 and 36, Member Economies are encouraged to educate one another in issues related to privacy protection and to share and exchange information on promotional, educational and training programs for the purpose of raising public awareness and enhancing understanding of the importance of privacy protection and compliance with relevant laws and regulations.

42. Member Economies are encouraged to share experiences on various techniques in investigating violations of privacy protections and regulatory strategies in resolving disputes involving such violations including, for instance, complaints handling and alternative dispute resolution mechanisms.

43. Member Economies should designate and make known to the other Member Economies the public authorities within their own jurisdictions that will be responsible for facilitating cross-border cooperation and information sharing between economies in connection with privacy protection.

II Cross-border Cooperation in Investigation and Enforcement

44. Developing cooperative arrangements: Taking into consideration existing international arrangements and existing or developing self-regulatory approaches (including those referenced in Part B. III., below), and to the

extent permitted by domestic law and policy, Member Economies should consider developing cooperative arrangements and procedures to facilitate cross-border cooperation in the enforcement of privacy laws. Such cooperative arrangements may take the form of bilateral or multilateral arrangements. This paragraph is to be construed with regard to the right of Member Economies to decline or limit cooperation on particular investigations or matters on the ground that compliance with a request for cooperation would be inconsistent with domestic laws, policies or priorities, or on the ground of resource constraints, or based on the absence of a mutual interest in the investigations in question.

45. In civil enforcement of privacy laws, cooperative cross-border arrangements may include the following aspects:

a) 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;

b) mechanisms for effectively sharing information necessary for successful cooperation in cross-border privacy investigation and enforcement cases;

c) mechanisms for investigative assistance in privacy enforcement cases;

d) 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;

e) steps to maintain the appropriate level of confidentiality in respect of information exchanged under the cooperative arrangements.

III. Cooperative Development of Cross-border Privacy Rules

46. Member Economies will endeavor to support the development and recognition or acceptance of organizations' cross-border privacy rules across the APEC region, recognizing that organizations would still be responsible for complying with the local data protection requirements, as well as with all applicable laws. Such cross-border privacy rules should adhere to the APEC Privacy Principles.

47. To give effect to such cross-border privacy rules, Member Economies will endeavor to work with appropriate stakeholders to develop frameworks or mechanisms for the mutual recognition or acceptance of such cross-border privacy rules between and among the economies.

48. Member Economies should endeavor to ensure that such cross-border privacy rules and recognition or acceptance mechanisms facilitate responsible and accountable cross- border data transfers and effective privacy protections without creating unnecessary barriers to cross-border information flows, including unnecessary administrative and bureaucratic burdens for businesses and consumers.

Asia-Pacific
Economic Cooperation

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]

---

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.

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

- 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).

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

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-bordertransfer to other participating 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 participantand will be enforceable by an appropriate authority, such as a regulator to ensure compliancewith 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*).

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.

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*).

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 takeholders' 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

11 http://webresources.apec.org/

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.

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 APECCross 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.