APEC

PRIVACY FRAMEWORK

Information flows are vital to conducting business in a global economy. The APEC Privacy Framework promotes a flexible approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows.

Asia-Pacific
Economic Cooperation

APEC

PRIVACY FRAMEWORK

Information flows are vital to conducting business in a global economy. The APEC Privacy Framework promotes a flexible approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows.

Asia-Pacific
Economic Cooperation

Published by

APEC Secretariat, 35 Heng Mui Keng Terrace, Singapore 119616
Tel: (65) 6775 6012 Fax: (65) 6775 6013
Email: info@apec.org Website: www.apec.org

ISBN 981-05-4471-5
APEC#205-SO-01.2

FOREWORD

APEC member economies realize the enormous potential of electronic commerce to expand business opportunities, reduce costs, increase efficiency, improve the quality of life, and facilitate the greater participation of small business in global commerce. A framework to enable regional data transfers will benefit consumers, businesses, and governments. Ministers have endorsed the APEC Privacy Framework, recognizing the importance of the development of effective privacy protections that avoid barriers to information flows, ensure continued trade, and economic growth in the APEC region.

part i. preamble

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.

1 The 1980 OECD Guidelines were drafted at a high level that makes them still relevant today. In many ways, the OECD Guidelines represent the international consensus on what constitutes honest and trustworthy treatment of personal information.

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.

part ii. scope

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

Definitions

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

9. 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.

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

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

11. 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.

Application

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.

12. 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.

13. 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.

INFORMATION PRIVACY PRINCIPLES

Asia-Pacific
Economic Cooperation

part iii. APEC information privacy principles

PRINCIPLES	COMMENTARY
I. Preventing Harm	
14. Recognizing the interests 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.	14. 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 protections, including self-regulatory efforts, education and awareness campaigns, laws, regulations, and enforcement mechanisms, 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 or 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.

PRINCIPLES

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:

    a) the fact that personal information is being collected;

    b) the purposes for which personal information is collected;

    c) the types of persons or organizations 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.

COMMENTARY

15-17. 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 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

PRINCIPLES

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.

COMMENTARY

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.

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

PRINCIPLES

COMMENTARY

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.

PRINCIPLES

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.

COMMENTARY

18. 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. Therefore, even in those economies where there is no explicit law against these specific methods, they may be considered an unfair means of collection.

PRINCIPLES

COMMENTARY

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:

    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,

19. 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. The fundamental criterion in

PRINCIPLES

c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.

COMMENTARY

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.

20. 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

PRINCIPLES

COMMENTARY

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.

PRINCIPLES

COMMENTARY

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 a mechanism to exercise choice, as in

PRINCIPLES

COMMENTARY

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.

21. 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

PRINCIPLES

COMMENTARY

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 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.

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

PRINCIPLES

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.

COMMENTARY

23-25. 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 by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access.

Access must be provided in a reasonable manner and form. A reasonable manner should include the normal methods of interaction between organizations and

PRINCIPLES

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.

COMMENTARY

individuals. For example, if a computer was involved in the transaction or request, and the individual's 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

PRINCIPLES

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.

COMMENTARY

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

PRINCIPLES

COMMENTARY

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 information that an organization has taken steps 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 to separate 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 an explanation as to why it has made that

PRINCIPLES

COMMENTARY

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.

26. 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

PRINCIPLES

COMMENTARY

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 a 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 the Framework 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;

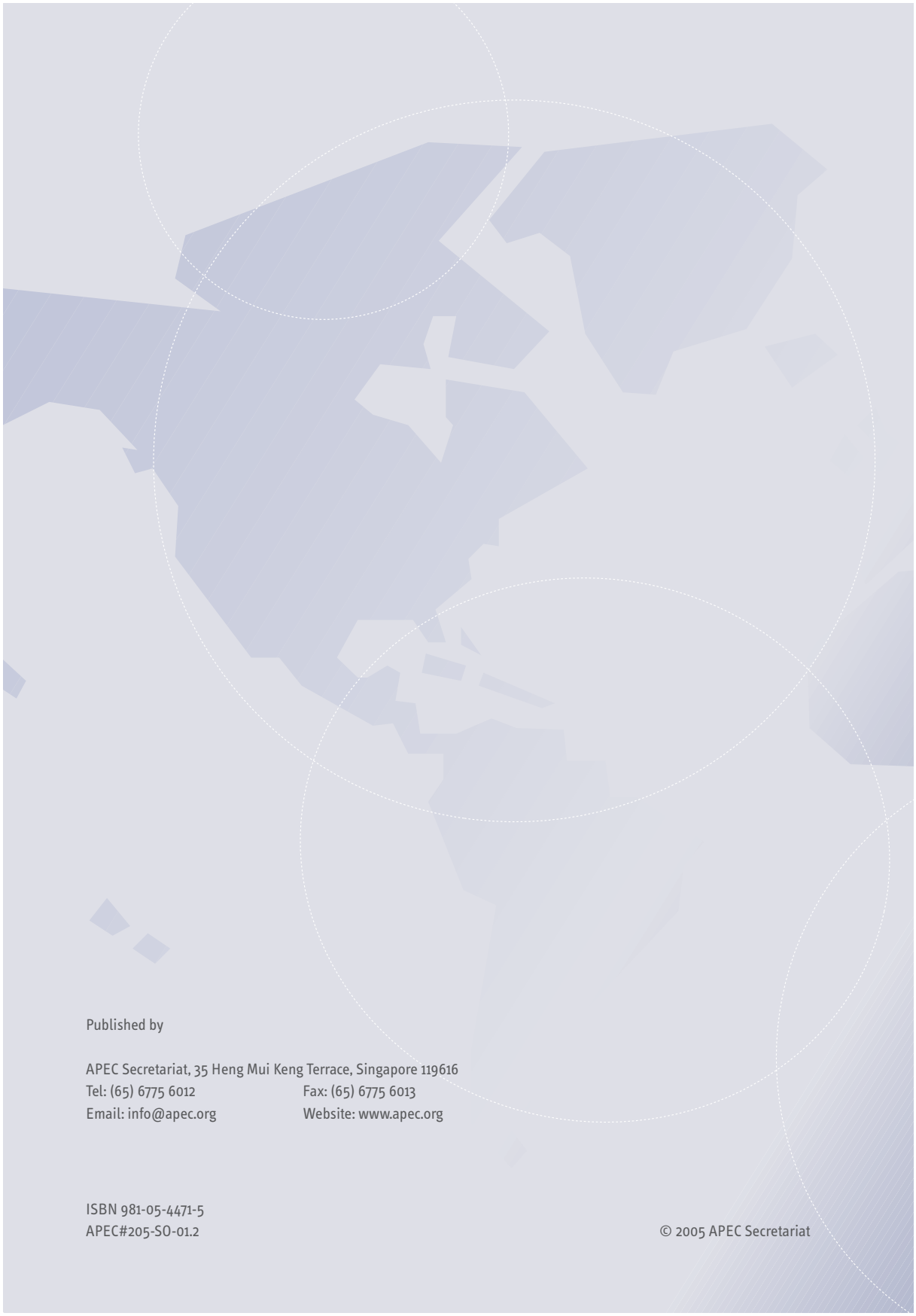
    e) steps to maintain the appropriate level of confidentiality in respect of information exchanged under the cooperative arrangements.

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.



Published by

APEC Secretariat, 35 Heng Mui Keng Terrace, Singapore 119616
Tel: (65) 6775 6012 Fax: (65) 6775 6013
Email: info@apec.org Website: www.apec.org

ISBN 981-05-4471-5
APEC#205-SO-01.2