APEC PRIVACY FRAMEWORK (2015)

CONTENTS

APEC PRIVACY FRAMEWORK (2015)

Foreword

APEC member economies realize the enormous potential of the digital economy to continue 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 protect privacy within and beyond economies and to enable regional transfers of personal information benefits 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 and ensure continued trade and economic growth in the APEC region.

Part I. Preamble

1. APEC economies recognize the importance of protecting information privacy while 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…". Consumer trust and confidence in the privacy and security of online transactions, information networks and management of personal information is critical in enabling member economies to reap the benefits of electronic commerce and participate in today's information-driven economy. APEC economies realize that a key part of efforts to improve consumer confidence and ensure the growth of electronic commerce and innovation must be cooperation to promote both effective information privacy protection and the free flow of information in the Asia Pacific region, while respecting domestic laws and regulations, applicable international frameworks for information privacy protection, and strengthening information security 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 deliver social and economic benefits for individuals, governments, businesses and society at

large, including increased consumer choice, market expansion, productivity, education, communication and product innovation. However, while these technologies make it easier and cheaper to collect, analyze and use large quantities of information, the way they are designed and used often make these activities undetectable to individuals. 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 use and 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. Business operations and consumer expectations have undergone a major shift due to changes in technology and the nature of information flows: businesses and other organizations now require simultaneous input and access to data 24-hours a day in order to meet business, 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, economies and individuals. Therefore, in promoting and enforcing ethical information practices, there is also a need to develop systems for protecting privacy that account for these 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 privacy protections and ensuring the free flow of information in the Asia Pacific region.

5. The Framework, which aims at promoting electronic commerce throughout the Asia Pacific region, is consistent with the core values of the OECD's Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (OECD Guidelines), and reaffirms the value of privacy to individuals and to the information society. The previous version of the Framework (2005) was modelled upon the OECD Guidelines (1980) which at that time represented the international consensus on what constitutes fair and trustworthy treatment of personal information. The updated Framework (2015) draws upon concepts introduced into the OECD Guidelines (2013)[1] with due consideration for the different legal features and context of the APEC region.

6. The Framework specifically addresses the importance of protecting privacy while maintaining information flows, as well as issues of particular relevance to APEC member economies. Its practical and distinctive approach is to focus attention on

[1] www.oecd.org/internet/ieconomy/privacy-guidelines.htm

consistent rather than identical privacy protection. In so doing, it seeks to reconcile privacy with business and societal 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 and government entities in APEC economies on common privacy issues and the impact of privacy issues upon the way legitimate business practice and government functions are to be conducted. It does so by highlighting the reasonable privacy expectations of the modern consumer. Businesses and member economies should respect individuals' privacy interests in a way that is consistent with the Principles outlined in the Framework.

8. The Framework was developed and updated in recognition of the importance of:

   - Implementing appropriate privacy protections for personal information, particularly from the harmful consequences of intrusions and the misuse of personal information;

   - The free flow of information to trade, and to economic and social growth in both developed and developing market economies;

   - Enabling global companies 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;

   - Empowering Privacy Enforcement Authorities to fulfill their mandate to protect individual privacy;

   - Advancing international and regional mechanisms, including the APEC Cross Border Privacy Rules (CBPR) system, to promote and enforce privacy and to maintain the continuity of information flows among APEC economies and with their trading partners;

   - Encouraging organizations to be accountable for all personal information under their control; and

   - Promoting interoperability between the Framework, and its implementing measures such as the CPEA and CBPR system, and privacy arrangements in other regions.

Part II. Scope

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

COMMENTARY

Core definitions

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

9. The Framework is intended to apply to information about natural living persons, not legal persons. The 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. For example, certain types of metadata, when aggregated, can reveal personal information and can give an insight into an individual's behavior, social relationships, private preferences and identity

10. **Personal information controller** means a person or organization who controls the collection, holding, processing, use, disclosure or transfer 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

10. The 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. For the purposes of the 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.

excludes an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.

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 that 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 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.

Additional definitions

12. **CBPR system** is the abbreviation of the APEC Cross Border Privacy Rules system.[2]

12. The APEC Cross Border Privacy Rules system, endorsed by APEC Leaders in 2011, is a voluntary accountability-based scheme to facilitate privacy-respecting personal information flows among APEC economies. It has four main components:
    - set criteria for bodies to become recognised as CBPR system Accountability Agents;
    - a process for information controllers to be certified as APEC CBPR system

[2] For more information see: www.cbprs.org

compliant by a recognised Accountability Agent;
- assessment criteria for use by recognised Accountability Agents when reviewing whether an information controller meets CBPR system requirements; and
- arrangements for enforcing CBPR system requirements through complaints processes provided by recognised Accountability Agents backed up by a Privacy Enforcement Authority (PEA) that is a participant in the CPEA.

13. **CPEA** is the abbreviation of the APEC Cross-border Privacy Enforcement Arrangement which is a practical multilateral mechanism which enables Privacy Enforcement Authorities to cooperate in cross-border privacy enforcement by creating a framework under which authorities may, on a voluntary basis, share information and request and render assistance in certain ways.[3]

13. The CPEA is a multilateral mechanism which enables Privacy Enforcement Authorities in the APEC region to cooperate in cross-border privacy enforcement of Privacy Laws. Any Privacy Enforcement Authority in an APEC member economy may participate. The CPEA aims to:
- facilitate information sharing among Privacy Enforcement Authorities in APEC member economies;
- provide mechanisms to promote effective cross-border cooperation between Privacy Enforcement Authorities in the enforcement of Privacy Law; and
- encourage information sharing and cooperation on privacy investigation and enforcement with privacy enforcement authorities outside the APEC region.

[3] The CPEA's formal title is "APEC Cooperation Arrangement for Cross-border Privacy Enforcement". For more information see: www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx

14. **Privacy Enforcement Authority** means any public body that is responsible for enforcing Privacy Law, and that has powers to conduct investigations and/or pursue enforcement proceedings.[4]

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

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

15. Privacy Laws in APEC member economies come in a variety of forms. Some are general privacy or data protection statutes while others take a sectoral approach covering particular areas such as credit reporting or health information. In some cases the relevant legal provisions are contained within broader laws dealing with such issues as telecommunications or consumer protection. It is not important for the purposes of the definition what the laws are called: it is the effect of the laws that matters.

16. **PRP system** is the abbreviation of the APEC Privacy Recognition for Processors system.

16. The PRP system represents the baseline requirements a processor must meet in order to be recognized by an APEC-recognized Accountability Agent and provide assurances with respect to the processor's privacy policies and practices. The PRP system helps personal information processors to demonstrate their ability to provide effective implementation of a personal information controller's privacy obligations related to the processing of personal information.

Application

17. In view of the differences in social, cultural, economic and legal backgrounds of each member economy, there should be flexibility in implementing these Principles.

17. Although it is not essential for electronic commerce that all laws and practices within APEC be identical, compatible approaches to privacy protection among APEC economies will greatly facilitate international commerce and privacy enforcement cooperation. Nonetheless, the Framework recognizes the need also to take into account social, cultural and other differences among economies.

18. 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.

18. Economies implementing the Framework at a domestic level may adopt suitable exceptions that suit their particular domestic circumstances.

    While recognizing the importance of governmental respect for privacy, the Framework is not intended to impede governmental actions authorized by law when taken to protect national security, public safety, national sovereignty or achieve other important public policy objectives. Nonetheless, member economies should endeavor to ensure that the impact of these activities upon the rights, responsibilities and legitimate interests of individuals and organizations is as limited as possible.

Part III. APEC Information Privacy Principles

19. The Information Privacy Principles should be viewed and interpreted as a whole rather than looking at particular principles in isolation as there is a close inter-relationship.[5]

PRINCIPLES	COMMENTARY
I. Preventing Harm	
20. 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.	20. This Principle recognizes that one of the primary objectives of the 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, organizational controls 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, use or transfer of personal information. Where there has been a significant security breach affecting personal information, it may help to reduce the

[5] There may be some minor inconsistency in language usage between principles (e.g. in relation to how the principles describe the use of personal information). A future revision project that includes the wording of the principles within its scope might usefully align the language. In the meantime, unless the context suggests otherwise, 'use' of personal information should be considered to include collection, holding, processing, use, disclosure or transfer of personal information.

risk of harmful consequences to the individuals concerned to give notice to Privacy Enforcement Authorities and/or the individuals concerned.[6]

II. Notice

21. 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.

21-23. This 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.

Depending on the context in which the personal information is collected, notice may be provided using various methods. For example, one common method of compliance with this Principle is for personal information controllers to post notices on their websites. Where organizations engage individuals in offline settings, such as in person or via the telephone, posted or written notices or telephone scripts may be used. In other situations, placement of notices on intranet sites or in employee handbooks, for example, may be appropriate. There are practical challenges to giving notice in the mobile context. To provide notice on small screens, personal information controllers may want to consider the value of standard notices, icons, or other measures.

[6] See clause 54 below.

22. 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.

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

Organizations should 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 digital 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 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 to be given notice regarding the collection and normal use of that information for expected business purposes.

Further, if colleagues who work for the same company as an 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

24. 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.

24. This Principle limits collection of personal information by reference to the purposes for which it is collected. The collection of the personal information should be relevant to such purposes, and necessity and proportionality to the fulfillment of such purposes may be factors 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 phishing, telemarketing calls, or pretexting emails 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 of collection, they may be considered to be 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 inform them of the potential health risk.

IV. Uses of Personal Information

25. 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,

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

25. This 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 personal information, the context of collection, the individual's expectations and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" 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

26. 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.

26. 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. 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, consideration should be given to tailoring the information and the way it is conveyed to make it more "easily understandable" to particular groups of individuals (e.g., by providing explanations in relevant languages, if the information is aimed at children, in ways that are age-appropriate).

    This Principle also recognizes, through the introductory words "where appropriate", that there are certain situations where it would not be necessary to provide a mechanism to exercise choice.

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 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 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 provide a mechanism to exercise choice related to the use of 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

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

27. This Principle recognizes that a personal information controller is obliged to maintain the accuracy and completeness of records and keep them up to date as necessary to fulfill the purposes of use. Making decisions about individuals based on inaccurate, incomplete or out of date information may not be in the interests of individuals or organizations.

VII. Security Safeguards

28. 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.

28. This Principle recognizes that individuals whose personal information is entrusted to others are entitled to expect that their information be protected with reasonable security safeguards.

VIII. Access and Correction

29. Individuals should be able to:

    a) obtain from the personal information controller confirmation of whether or not the personal information

29-31. 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

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 personal information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.

30. 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

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 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

individual would be violated.

31. 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.

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 must 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 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 determination and information on how to challenge that denial. An organization would not be expected to provide an explanation in cases where such explanation would violate a law or judicial order.

IX. Accountability

32. 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.

32. 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.

    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.

    A useful means for a personal information controller to help ensure accountability for the personal

information it holds is to have in place a privacy management programme.[7]

Part. IV. Implementation

33. 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

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

I. Maximizing Benefits of Privacy Protections and Information Flows

35. Personal information should be collected, held, processed, used, transferred, and disclosed in a manner that protects individuals' privacy and allows individuals and economies to maximize the benefits of information flows within and across borders.

36. Consequently, as part of establishing or reviewing their privacy protections to give effect to the APEC Privacy Framework, member economies 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

37. 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 policy instruments. In practice, the Framework

[7] See clauses 43-45 below.

is meant to be implemented in a flexible manner that can accommodate various models of enforcement, including through Privacy Enforcement Authorities, multi-agency enforcement bodies, a network of designated industry bodies, courts and tribunals, or a combination of the above, as member economies deem appropriate.

38. The means of giving effect to the Framework will often differ between member economies. An individual member economy may determine that different Information Privacy Principles call for different means of domestic implementation. Whatever approach is adopted in a particular circumstance, the overall goal should be to develop compatible privacy protection approaches in the APEC region that are respectful of individual economies' requirements.

39. APEC economies should adopt non-discriminatory practices in giving effect to the Framework's principles and in protecting individuals from privacy protection violations occurring in that member economy's jurisdiction. [For example, member economies should ensure that laws or other approaches that give effect to the protections in the Framework do not impede individuals living in other economies from benefitting from those protections.

40. Coordination across government agencies and other stakeholders is important to identify ways to strengthen privacy without creating obstacles to national security, public safety, and other public policy objectives.

41. Member economies should consider establishing and maintaining Privacy Enforcement Authorities. Privacy Enforcement Authorities that are established should be provided with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis.

42. Privacy Enforcement Authorities may find it useful to apply a risk-based approach to selected oversight efforts and, where permitted, to prioritize their enforcement efforts according to the likelihood and severity of harm that might result from privacy violations or from an action taken or proposed.[8]

[8] See the Preventing Harm Principle.

III. Privacy Management Programmes

43. An operative privacy management programme will provide a sound basis for a personal information controller to demonstrate that it is complying with measures that give effect to the privacy protections in the Framework.

44. Accordingly, member economies should consider encouraging personal information controllers to develop and implement privacy management programmes for all personal information under their control. Privacy management programmes should:

    a) be tailored to the structure and scale of the operations of the personal information controller, as well as the volume and sensitivity of the personal information under its control;
    b) provide appropriate safeguards based upon risk assessment that takes into account the potential harm to individuals;
    c) establish mechanisms for internal oversight and response to inquiries and incidents;
    d) be overseen by designated accountable and appropriately trained personnel; and
    e) be monitored and be regularly updated.

45. Personal information controllers should be prepared to demonstrate their privacy management programmes at the request of a competent Privacy Enforcement Authority of that economy or in response to a valid request by another appropriate entity, such as an accountability agent designated under the CBPR system or under an industry code of conduct giving effect to the Framework.

IV. Promotion of technical measures to protect privacy

46. Technical measures can make a significant contribution to the overall effectiveness and impact of domestic privacy regimes, by supplementing and complementing legal protections of privacy. Therefore, when considering approaches to give effect to the Framework, member economies should promote technical measures which help to protect privacy.

47. Member economies may, for example, encourage personal information controllers to make full use of readily available technical safeguards and measures. In addition, they may promote research and development, encourage further privacy innovation and

support the development of technical standards that embed best privacy practice into systems engineering.

V. Public education and communication

48. For the Framework to be of practical effect, it must be known and accessible. Accordingly, member economies should:

    a) publicize how their Privacy Laws and other domestic arrangements provide privacy protections to individuals;

    b) engage in activities that raise awareness amongst:

        i. personal information controllers about the economy's privacy protections and the controllers' responsibilities;

        ii. Personal information processors about practices that help provide effective implementation of a personal information controller's privacy obligations related to the processing of personal information; and,

        iii. individuals about how they can report violations and how remedies can be pursued; and

    c) Encourage or require Privacy Enforcement Authorities and other bodies having responsibilities to administer privacy protections established at domestic level (for example, CBPR system accountability agents or bodies established to give effect to self-regulatory schemes) to report publicly on their activities where appropriate.

VI. Cooperation within and between the Public and Private Sectors

49. Active participation of non-governmental entities will help ensure that the full benefits of the Framework can be realized. Accordingly, member economies should engage in a dialogue with relevant non-government stakeholders, including those representing citizens, consumers and industry and technical and academic communities, to obtain input on privacy protection and information flow issues and to seek cooperation in furthering the Framework's objectives. Furthermore, member economies that have not yet established domestic privacy protection regimes should pay ample attention to the interests and needs of non-government stakeholders when developing privacy protections.

50. Member economies should seek the cooperation of non-governmental entities such as those representing citizens and consumers in raising public awareness about privacy protection issues. As well, member economies should encourage these entities to actively engage in promoting and supporting the privacy interests of individuals, for example by referring complaints to Privacy Enforcement Authorities and publicizing the outcomes of those complaints.

51. Member economies should consider developing strategies that reflect a coordinated approach to implementing privacy protections across governmental bodies.

52. Member economies should also consider undertaking consultation and capacity building efforts across the public and private sectors, and with non-government stakeholders, including, for example, by:

    a) developing or supporting networks of individuals responsible for privacy compliance within organizations; and

    b) producing informational materials and arranging experience sharing events.

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

53. A member economy's system of privacy protections should include appropriate remedies for privacy violations, which could include redress, the ability to stop a violation from continuing, and other remedies. In determining the range of remedies for privacy violations, member economies should take a number of factors into account 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.

54. A member economy should consider encouraging or requiring personal information controllers to provide notice, as appropriate, to Privacy Enforcement Authorities and/or other relevant authorities in the event of a significant security breach affecting personal information under its control. Where it is reasonable to believe that the breach is likely to affect individuals, timely notification directly to affected individuals should be encouraged or required, where feasible and reasonable.

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

55. 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

56. 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

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

58. 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.

59. 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.

60. 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.

61. Member economies should encourage the development of internationally comparable metrics to inform the policy making process relating to privacy and personal information flows.

II. Cross-border cooperation in investigation and enforcement

62. Taking into consideration existing international arrangements (including the CPEA) and existing or developing self-regulatory or co-regulatory approaches, and to the extent permitted by domestic law and policy, member economies should expand their use of existing cooperative arrangements and consider developing additional cooperative arrangements or procedures, as necessary, to facilitate cross-border cooperation in the enforcement of privacy laws. Such cooperative arrangements may take the form of bilateral or multilateral arrangements.

63. The preceding 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.

64. 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 initiatives that target conduct that is inconsistent with the protections set forth in the Framework and that may affect individuals or personal information controllers in those other 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 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. Cross-border privacy mechanisms

65. APEC recognized the importance of protecting privacy while maintaining the free flow of personal information across borders and has encouraged member economies to implement the Framework to provide conditions in which information can flow safely and accountably, for instance through the use of the CBPR system.

66. Member economies will endeavor to support the development and recognition or acceptance of cross-border privacy mechanisms for use by organizations to transfer personal information across the APEC region, recognizing that organizations would still be responsible for complying with the local privacy requirements, as well as with all applicable laws. Such mechanisms should apply the APEC Information Privacy Principles.

67. To give effect to paragraph 65, member economies have developed the CBPR system[9], which provides a practical mechanism for participating economies to implement the APEC Privacy Framework in an international, cross-border context, and to provide a means for organizations to transfer personal information across borders in a manner in which individuals may trust that the privacy of their personal information is protected.

68. Member economies worked with appropriate stakeholders to develop the PRP system to complement the CBPR system to help personal information processors demonstrate their ability to provide effective implementation of a personal information controller's obligations related to the processing of personal information.

[9] The 2011 Leaders Declaration states "We will take the following steps to further open markets and facilitate regional trade: […] implement the APEC CBPR to reduce barriers to information flows, enhance consumer privacy, and promote interoperability across regional data privacy regimes." (http://www.apec.org/Meeting-Papers/Leaders-Declarations/2011/2011_aelm.aspx)

IV. Cross-border transfers

69. A member economy should refrain[10] from restricting cross border flows of personal information between itself and another member economy where (a) the other economy has in place legislative or regulatory instruments that give effect to the Framework or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures (such as the CBPR) put in place by the personal information controller to ensure a continuing level of protection consistent with the Framework and the laws or policies that implement it.

70. Any restrictions to cross border flows of personal information should be proportionate to the risks presented by the transfer, taking into account the sensitivity of the information, and the purpose and context of the cross border transfer.

V. Interoperability between privacy frameworks

71. Recognizing that personal information flows do not stop at regional boundaries, member economies should encourage and support the development of international arrangements that promote interoperability amongst privacy instruments that give practical effect to this Framework.

72. Improving the global interoperability of privacy frameworks can bring benefits in improved personal information flows, help ensure that privacy requirements are maintained when personal information flows beyond member economies and can simplify compliance for personal information controllers and processors. Global interoperability can also assist individuals to assert their privacy rights in a global environment and help authorities to improve cross-border privacy enforcement.

[10] Cross border data flows remain subject to member economies applicable domestic laws, regulations, and international agreements and commitments.