# APEC 隱私保護綱領

## 第一章　前言

1. APEC 經濟體已體認到保護資訊隱私與維持亞太地區經濟體間及其貿易夥伴間之資訊流通的重要性。當 APEC 部長認可 1998 電子商務行動計劃(1998 Blueprint for action on electronic commerce)時，已體認到電子商務的實踐必須倚賴政府部門與民間私部門共同努力合作發展技術與政策並共同執行之，該等技術與政策必須能夠建立起一套安全、保密且可信賴的通訊、資訊與傳輸系統並相當著重於隱私等議題。如果消費者對線上交易及資訊網路之安全性和隱私保護缺乏信賴，那麼各會員勢必難以發展其電子商務。APEC 經濟體深刻地體認到增進消費者的信賴以及確保電子商務的成長的重要關鍵乃在於整合並促成有效率的資訊隱私保護以及亞太地區資訊的自由流通。

2. 網際網路和其他資訊網路連結的資訊及通訊科技的發展，包括行動科技在內，使得人們得以隨時隨地的搜集、儲存和利用資訊。這些科技的發明為企業、個人及政府帶來極大的社會和經濟利益，包括消費選擇的增加、市場的擴張、生產力的提昇、教育及產品的創新。雖然此些科技使得大量資訊的搜集、連結和利用變得更加便捷以及成本變得更低，但另一方面，此些科技的利用也使個人不更易察覺該等活動。結果將是個人不易維持其對個人資訊隱私的控制。因此，為了提升個人及企業的信賴感，將有必要增進線上及非線上資訊的利用倫理以及養成可信賴的資訊行為。

## APEC PRIVACY FRAMEWORK

# 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. 當企業組織及消費者的期待皆隨著科技的變遷以及資訊流動的特質而持續變化時，企業和他種類型的組織為了符合客戶及社會需求並提供其有效率且節省成本的服務，將必須每天 24 小時都能同步存取資料。非必要性地限制或加諸任何負担於此種資訊流動需求的法規綱領將會對全球性的商業經濟造成負面影響。因此，於增進資訊利用倫理之際，將有必要發展一套可以保護與全球經濟發展現實息息相關的資訊隱私制度。

4. APEC 經濟體支持此一原則性的 APEC 隱私保護綱領(APEC Privacy Framework)以做為提升資訊隱私保護的重要工具並確保亞太地區間資訊的自由流動。

5. 此綱領旨在推廣亞太地區的電子商務，乃是與 OECD 的 1980 年隱私保護及個人資料之國際傳遞指導方針[1](1980 Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data )的核心價值相符，並且再次確立了隱私之於個人和資訊社會的價值。

6. 此一保護綱領特別著重於這些基本概念以及和 APEC 會員經濟體特別相關的議題。其特別之處在於其著重於實務運作以及與此一脈絡相一致的資訊隱私保護。如此一來，其平衡了資訊隱私、企業需求和商業利益，亦同時調和了存於各會員經濟體間的文化及其他各種差異性。

7. 此一保護綱領主要就一般性的隱私議題及隱私議題對於企業行為的影響，提供 APEC 經濟體內的企業組織一清楚明白的指導與方向。突顯現代消費者的合理隱私期待，使企業組織在符合本綱要所提列之各項原則的情況下認知到消費者的隱私利益。

[1] 由於 1980 經濟合作發展組織指導方針制定時已具有很高的水準，故仍能適用於今日。在很多方面，經濟合作發展組織指導方針象徵著國際間對於個人資訊如何制定公正且值得信賴的處理方式，已有一致共識。

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

4. APEC economies endorse the principles-based APEC Privacy Framework as an important tool in encouraging the development of appropriate information privacy protections and ensuring the free flow of information in the Asia Pacific region.

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

6. The Framework specifically addresses these foundation concepts, as well as issues of particular relevance to APEC member economies. Its distinctive approach is to focus attention on practical and consistent information privacy protection within this context. In so doing, it balances information privacy with business needs and commercial interests, and at the same time, accords due recognition to cultural and other diversities that exist within member economies.

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

[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.

8. 最後，此一隱私保護綱領乃是 APEC 在體認到下列事項的重要性的情況下所發展出來的：

- 發展適當的隱私保護措施，防止個人資訊因不經本人同意而遭取用所造成的不利影響以及避免個人資料遭到濫用；

- 體認到資訊的自由流動是促成已開發和開發中國家之經濟和社會持續成長的一項重要因素；

- 促使於 APEC 會員經濟體內蒐集、存取、利用或處理個人資料的全球性組織在其組織內部發展並執行一套有關個人資料存取和利用的全球化標準程序；

- 促使執行機關全力實施其所制定的法令以保護資訊隱私；以及

- 增進跨國機制以提升及執行資訊隱私並維持 APEC 會員經濟體間及其貿易夥伴間資訊的持續流動。

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.

| 原則 | 說明 |
| --- | --- |

# 第二章. 範圍

APEC 隱私保護綱領第二章旨在說明隱私保護原則的適用範圍。

## 定義

| | |
| --- | --- |
| 9. 個人資料指任何關於可識別個人或足資識別該個人之資料。 | 9. 此一保護綱領是在有些經濟體已發展出良好的隱私保護法制或是慣例，有些經濟體正考量制定相關隱私保護法制的背景下建立的。該等已建立隱私保護法制之經濟體對於個人資料之定義未必完全相同。 例如有些國家會將個人資料區分為可立即搜尋而得的資料和其他資料。雖然各經濟體的隱私保護法制間存有差異性，但 APEC 隱私保護綱領期望能夠使 APEC 經濟體間的隱私保護法制趨於一致。<br><br>此一保護綱領主要適用於自然人之個人資料保護，並不適用於法人。APEC 隱私保護綱領所稱的個人資料乃是該等可以識別個人的資料。但是，此亦包括了不能用以識別個人，但經過串檔之後得以識別該個人之資料。 |

| PRINCIPLES | COMMENTARY |
| --- | --- |

# 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.<br><br>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. |

| 原則 | 說明 |
| --- | --- |
| 10. 個人資料管理者(personal information controller )指蒐集、持有、處理或利用個人資料之個人或機構，包括授權他人代為蒐集、持有、處理、利用、傳遞或揭露個人資料者，但不包括受他人指示而為上列行為者，亦不包括因個人之私人、家庭因素而蒐集、持有、處理或利用個人資料者。 | 10. APEC 隱私保護綱領適用於蒐集、持有、處理、利用、傳遞或揭露個人資料之公務機關和非公務機關(包括個人和機構)。各經濟體對於個人資料管理者的定義並不完全相同。但是，基於本綱領之目的，APEC 經濟體同意當個人或機構授權他人代為蒐集、持有、處理、利用、傳遞或揭露個人資料時，該個人或機構亦稱之為個人資料管理者，需遵行本綱領所訂立的隱私保護原則。<br><br>個人經常會因為私人或家庭事務而蒐集、持有和利用個人資料。例如，個人常會持有通訊薄和電話薄或是從事於家庭事務的聯絡(prepare family newsletters)。APEC 隱私保護綱領並不欲適用於此種狀況。 |
| 11. **公開可獲得之資料(publicly available information )**指當事人明示同意公開或是經由下列合法途徑取得的個人資料：<br>a) 合法公開之政府檔案；<br>b) 新聞報導；或<br>c) 依法公開之個人資料。 | 11. APEC 隱私保護綱領對於公開可獲得之資料亦有所規範。告知及選擇的規定(Notice and choice requirements)是不必要的，尤其是在資料是處於公開可獲得以及個人資料管理者非直接地從相關個人取得資料。公開可獲得之資料可能隱含於公眾可獲得的政府檔案中，例如選舉人名冊，或是隱含於新聞媒體所發行或所播報的新聞中。 |

| PRINCIPLES | COMMENTARY |
| --- | --- |
| 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.<br><br>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:<br><br>a) government records that are available to the public;<br><br>b) journalistic reports; or<br><br>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. |

| 原則 | 說明 |
| --- | --- |
| **適用** | |
| 12. 基於各會員經濟體間的社會、文化、經濟和法律的差異性，應彈性地執行此一保護綱領所訂立的原則。 | 12. 雖然就電子商務的發展而言，APEC 會員經濟體的法律制度和慣例，包括個人資料的定義在內並不需完全相同，但是各 APEC 經濟體的隱私保護法制如果具有相容性將有助於國際商務的發展。APEC 隱私保護綱領所訂立的原則已考量到上述的情況，但是亦考量到各經濟體間的文化、社會、經濟等差異性。因此，對於隱私保護制度的設計將著眼於對國際商務而言最重要者。 |
| 13. 定於本綱領第三章的隱私保護例外原則，包括與國家主權、國家安全、公共安全和公共政策相關者，在適用上應：<br>a) 限縮於與例外條款相關之目的並符合比例原則；以及<br>b) (i) 為公眾所知悉；或<br>(ii) 符合法律規定。 | 13. 定於本綱領第三章的隱私原則在解釋上應從整體綱領為之，而非各別論之，因各項原則間具有密切的相關性。例如利用原則(Use Principle)與告知和選擇原則(Notice and Choice Principles)密切相關。各經濟體於其境內得採取適切於其國內環境的例外條款。<br>雖然體認政府尊重個人隱私的重要性，但是 APEC 隱私保護綱領並不欲凌駕於政府基於國家安全、公共安全、國家主權和其他公共政策的原因而依法採取的措施之上。雖然如此，各經濟體應要考量此等措施對於個人和機構之權利、義務和法益的影響。 |

| PRINCIPLES | COMMENTARY |
|---|---|
| **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:<br>a) limited and proportional to meeting the objectives to which the exceptions relate; and,<br>b) (i) made known to the public; or,<br>(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.<br>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. |

| 原則 | 說明 |
| --- | --- |

# 第三章. APEC 資訊隱私保護原則

## I. 預防損害

| | |
| --- | --- |
| 14. 基於個人合理的隱私期待，個人資訊隱私保護制度的設計應要著眼於防止個人資訊遭到濫用。基於個人資料有可能遭到他人之濫用因而對個人造成損害，故應有適當的保護措施以防止此種損害的發生。其次，對於個人資料之蒐集、利用和傳遞所生的損害，應有適切的損害填補機制。 | 14. 預防損害原則為 APEC 隱私保護綱領的一個主要原則之一，其目的在防止個人資料遭到濫用以及因此所生的損害。因此，隱私保護，包括業者自律、教育及以告知為目的的各種宣傳、法律、命令以及各種執行機制等應要著眼於防止個人資料遭到他人的不當蒐集以及濫用。依此，關於相關的損害填補機制應要著眼於防止因個人資料遭到不當蒐集或濫用所生的損害，並且適切於損害發生的可能性及嚴重程度。 |

PRINCIPLES COMMENTARY

# Part III. APEC Information Privacy Principles

## 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.

| 原則 | 說明 |
| --- | --- |
| **II. 告知** | |
| 15.個人資料管理者對於其所蒐集和持有的個人資料應要向當事人提供清楚且容易取得的隱私保護政策聲明，包括：<br><br>a) 個人資料已遭蒐集的事實聲明；<br><br>b) 蒐集個人資料的目的；<br><br>c) 揭露個人資料的對象；<br><br>d) 個人資料管理者的身份及位址，包括如何和個人資料管理者聯絡有關於其隱私保護政策以及如何處置個人資料的資料；<br><br>e) 關於當事人得以請求查閱、閱閱、更正和限制其個人資料之利用及揭露範圍的選擇和方法。<br><br>16.個人資料管理者應採取合理的措施以確保當事人於其個人資料遭蒐集前或蒐集時已知悉其隱私保護政策。此外，一旦個人資料管理者之隱私保護政策開始實行，應立即告知當事人關於此一保護政策。<br>（繼續） | 15-17. 告知原則是要確保當事人能夠知悉其個人資料已遭蒐集以及個人資料的利用目的。藉由此一隱私保護聲明之提供，當事人可以更詳確地取得與個人資料管理者互動的資訊。實行此一原則最簡便、普通方式乃是將隱私保護政策臚列於個人資料管理者的網站上。其他方法，例如將隱私保護政策置於內部網路的網站或員工手冊上都是可以的。<br><br>有關於隱私保護政策應於何時提供於當事人乃是由 APEC 會員經濟體所共同決定的。APEC 會員經濟體同意良好的隱私保護措施是在個人資料被蒐集前或蒐集時即告知當事人關於個人資料管理者的隱私保護政策。同時，有些情況確實無法於個人資料被蒐集前或蒐集時立即告知當事人有關於個人資料管理者的隱私保護政策，例如當事人自發性的行為造成電子科技自動地蒐集該當事人的個人資料，常見的情況是 cookies 的利用。<br><br>（繼續） |

| PRINCIPLES | COMMENTARY |
| --- | --- |
| **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:<br><br>a) the fact that personal information is being collected;<br>b) the purposes for which personal information is collected;<br>c) the types of persons or organizations to whom personal information might be disclosed;<br>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;<br>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.<br><br>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.<br>(continue) | 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.<br><br>The requirement in this Principle relating to when notice should be provided is based on a consensus among APEC member economies. APEC member economies agree that good privacy practice is to inform relevant individuals at the time of, or before, information is collected about them. At the same time, the Principle also recognizes that there are circumstances in which it would not be practicable to give notice at or before the time of collection, such as in some cases where electronic technology automatically collects information when a prospective customer initiates contact, as is often the case with the use of cookies.<br><br>(continue) |

| 原則 | 說明 |
| --- | --- |
| **II. 告知** | |
| （繼續）<br>17. 當個人資料管理者所蒐集及利用的個人資料為公開可獲得之個人資料時，本原則不適用之。 | （繼續）<br>15-17.<br>此外，當個人資料的取得非直接源自當事人本人，而時來自第三人時，亦不適於個人資料被蒐集前或蒐集時立即告知當事人有關於個人資料管理者的隱私保護政策。例如，當保險公司基於提供醫療保險服務之目的而蒐集員工之個人資料，該公司可能無法於於員工之個人資料被蒐集前或蒐集時立即告知員工有關於公司的隱私保護政。<br><br>除此之外，在有些情況下並無必要適用此一告知原則，例如蒐集及利用公開可獲得的資料、基於商業關係而取得的資料或是關於當事人之專業能力的資料。例如當事人基於商業往來之目的而給予他人名片，當事人並不能期待個人資料管理者對於此一名片上之個人資料的正常利用和蒐集有任合隱私保護政策的聲明與告知。<br><br>又例如，與當事人在同一家共事的同事如果基於商業往來之目的而將當事人之名片提供予潛在客戶時，當事人並不能期待該名同事需告知其有關於當事人之個人資料的傳遞與利用。 |

| PRINCIPLES | COMMENTARY |
| --- | --- |
| **II. Notice** | |
| (continue) | (continue) |
| 17. It may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information. | 15-17.<br>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.<br><br>Additionally, there are situations in which it would not be necessary to provide notice, such as in the collection and use of publicly available information, or of business contact information and other professional information that identifies an individual in his or her professional capacity in a business context. For example, if an individual gives his or her business card to another individual in the context of a business relationship, the individual would not expect that notice would be provided regarding the collection and normal use of that information.<br><br>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. |

| 原則 | 說明 |
| --- | --- |
| **III. 蒐集限制** | |
| 18. 個人資料之蒐集應限於與蒐集目的相關的範圍，依合法或正當方法為之，並在適切的情況下告知當事人或取得其同意。 | 18. 此原則將個人資料之蒐集限於與蒐集目的相關者。個人資料之蒐集應與蒐集目的間具有關連性，實現此一目的相關因素應可為決定何謂關連性的一項要件之一。<br><br>此原則亦要求資料的蒐集方法必須合法及正當。所以，如果以虛偽不實的方法取得個人資料(例如冒用他公司之名義，利用電話行銷、平面廣告、或電子郵件等工具，詐欺消費者或引誘其揭露該名消費者個人的信用卡號碼、銀行帳戶資料或其他敏感性的個人資料)在許多會員經濟體境內都是不合法的行為。此外，即便某些會員經濟體的法律並無針對上述之方法有明白的規範，但可能認為那是以不正當方法獲取個人資料。<br><br>在有些情況之下，並無法告知當事人或取得其同意。例如在食物中毒的情況下，為了告知消費者潛在的健康問題，衛生單位有必要在不告知當事人或不取得其同意的情況下，向餐廳蒐集個人資料。 |

| PRINCIPLES | COMMENTARY |
| --- | --- |
| **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. | 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.<br><br>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.<br><br>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. |

| 原則 | 說明 |
| --- | --- |
| **IV. 個人資料之利用** | |
| 19. 個人資料之利用僅限於與蒐集目的一致或相關的範圍內，但有下列情況，不在此限：<br><br>a) 取得當事人本人的同意；<br><br>b) 為提供當事人所要求之產品或服務所必要者;或<br><br>c) 法律明文規定者。 | 19. 利用原則規定個人資料之利用限於與蒐集目的一致或相關的範圍內。基於此原則之目的，「個人資料之利用」包括個人資料之傳遞或揭露。<br><br>於適用此原則時，需考量資訊的本質、資料蒐集之目的與資料之利用用途。判斷利用目的是否與聲稱的蒐集目的相關或相符的基本要件為是否個人資料的利用乃是基於或是有利於該目的的達成。個人資料的利用「與目的一致或相關」可以為擴張解釋，例如設計並利用資料庫使人力管理更有效率與便捷、由第三人負責員工薪資名冊的處理、或是利用基於授信之目的所蒐集之資料。 |

| PRINCIPLES | COMMENTARY |
| --- | --- |
| **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:<br><br>a) with the consent of the individual whose personal information is collected;<br><br>b) when necessary to provide a service or product requested by the individual; or,<br><br>c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect. | 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.<br><br>Application of this Principle requires consideration of the nature of the information, the context of collection and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" 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. |

| 原則 | 說明 |
| --- | --- |
| **V. 當事人自主** | |
| 20. 在情況允許的情況下，個人資料管理者應提供當事人可就其個人資料之蒐集、利用和揭露進行選擇的機制，該機制必須清楚明白、顯見易懂、可查閱和可負担的。當個人資料管理者所蒐集者為公開可獲得之資料時，本規定不適用之。 | 20. 選擇原則旨在確保當事人有機會就其個人資料的蒐集、利用、傳遞和揭露進行選擇。不論此一機制是以電子格式、書面或其他方式為之，資訊管理者都必須以文字明白清楚地說明此一機制。同時，此一機制需能為當事人所能查閱以及負担的。使用該機制的容易性及及方便性應納入考量。<br><br>當一個機構針對某一特定國家之人民量身訂做一套選擇機制時，該機制必須容易瞭解或是能為該特定國家之人民所能理解，例如需使用其所能閱讀之語言。但是，如果選擇機制不是只針對某一特定國家之人民或是只針對機構所在地的人民所提供時，此一要求並不適用。<br><br>透過「在情況允許的情況下」的要件的說明，表明我們知道在某些特定的情況下可以很明白地知道當事人會同意資料的蒐集、利用等，或是在某些的情況下選擇機制無適用上的必要性。<br><br>（繼續） |

PRINCIPLES

COMMENTARY

## 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 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.

(continue)

| 原則 | 說明 |
| --- | --- |
| **V. 當事人自主** | |
| | 20.（繼續）<br>如同於此原則中所指明的，APEC 會員經濟體同意當所蒐集的資料是公開可獲得的資料時候，可以不必有選擇機制的適用或是無法提供選擇機制。例如透過公開檔案或是報紙蒐集個人的姓名和地址時，沒有必要提供選擇機制於當事人。<br><br>除了上列涉及公開可獲得資料的蒐集的情況外，APEC 會員經濟體亦同意於蒐集、利用、傳遞或揭露其他種類的資訊時，在某些特定的情況下，可以不必提供選擇機制。例如，於社交場合因名片交換而取得的個人商業聯絡資料或關於該個人之專業能力的資料時，且該個人也預期其個人資料為因商業聯絡而被利用時，一般來說無法也無必要在此種情況下提供選擇機制予當事人。<br><br>其次，當僱主基於僱佣關係而利用員工之個人資料時，並無必要提供選擇機制予員工。例如，一個機構欲將其人力資源的資料集中化處理時 並不需要提供選擇機制予其員工。 |

PRINCIPLES

**V. Choice**

COMMENTARY

20. (continue)

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 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.

| 原則 | 說明 |
| --- | --- |
| **VI. 個人資料之完整性** | |
| 21. 個人資料應正確、完整並應依利用目的為必要之更新。 | 21. 此一原則說明個人資料的管理者有義務維持個人資料的正確性和完整性並更新個人資料。基於不正確、不完整或陳舊的個人資料而做出與當事人個人相關的判斷對於機構或當事人都是件不利益的事情。但本原則亦明白的表示個人資料管理者的義務僅止於利用目的之必要範圍內。 |
| **VII. 安全管理**<br>**Security Safeguards** | |
| 22. 個人資料管理者應妥善地保護個人資料之安全，例如防止他人未經授權不當地截取、利用、修改、或揭露個人資料或其它濫用個人資料之行為。個人資料管理者所採的保護措施應與濫用行為的發生機率和可能造成的傷害、個人資料的敏感度和內容成比例，並應定期檢視和重新評估該些保護措施。 | 22. 本原則旨在說明當事人對於其個人資料將受到安全的保護一事應有合理的期待。 |

| PRINCIPLES | COMMENTARY |
| --- | --- |
| **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 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. |

| 原則 | 說明 |
| --- | --- |
| **VIII. 查閱和更正** | |
| 23. 當事人應：<br>a) 可以自個人資料管理者取得有關於其是否持其個人資料的資訊；<br>b) 提供可逐茲識別的個人資料後，可以和個人資料管理者聯絡；<br>i 在合理期間內；<br>ii 若收費的話，不能高；<br>iii 以合理的方式；<br>iv 以般可理解之形式；和<br>c) 在適合及可能的狀況下，指正與當事人相關之個人資訊的正確性以及更正、補充或請求刪除該筆資料。 | 23-25. 就個人隱私的保護來說，查閱與更正個人資料並不是一個絕對的權利。本原則規定了在那些是必須提供個人查閱與更正個人資料的合理條件，包括時間、費用和提供個人查閱其個人資料的方式和形式。所謂的合理必須視個案而定，例如個人資料的處理方式。個人將受限於安全因素而無法直接查閱個人資料並需要証明其有需直接查閱個人資料的需要。<br>應以合理的方式及形式供個人可以查閱其個人資料。合理的方式應包括個人與機構間的正常互動。例如，如果是透過電腦提出請求，且具有個人電子郵件位址之資料，那麼電子郵件將會被視為提供資訊的合理方法。如果機構先前已回覆過個人之請求時，當個再次提出請求時，該機構得以利用和先前相同或相似之方式回覆個人的請求，或者機構可以以其機構內可提供之方法回覆個人之請求，但是不能有語言閱讀上的問題。<br>（繼續） |
| 24. 應提供個人查閱及更正其個人資料，除非有下列情形：<br>(i) 提供個人查閱其個人資料之成本或負擔明顯不合理，或與個案中個人隱私受到侵害之風險不成比例。<br>(ii) 基於法律或安全理由，或是為了保護商業秘密而不應揭露該資訊；或<br>(iii) 他人之資訊隱私會受到侵害。 | |
| 25. 如果拒絕在(a)或(b)的情況下所為的請求或是在(c)所為的指正，應提供個人有關於該請求或指正遭到拒絕之理由。 | |

## PRINCIPLES

### VIII. Access and orrection

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 derstandable; and,

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

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

    (i) the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question;

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

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

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

## 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 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.

(continue)

| PRINCIPLES | COMMENTARY |
| --- | --- |
| 原則 | 說明 |
| **VIII. 查閱和更正** | |
| | （繼續）<br>23-25.<br>對於複製個人資料和其他解說的請求，機構應以可理解之文本答覆之。但這不包括電腦語言的翻譯(例如僅有電腦可解讀的指令、原始碼或機械語言)。但是，如果某一個代碼代表了某種特定的意義，資料控制主體應向個人解釋之。例如，為機構所保有的個人資料包括了個人的年齡資料，且該年齡資料是以組距的方式呈現並由特定代碼表示之(例如1代表18-25歲，2代表26至35歲…等)，那麼當提供個人此代碼時，應向其解釋此代碼所表示的意義。<br><br>當個人提出查閱其個人資料之請求時，個人資料應以其紀錄狀態的語言呈現。當紀錄個人資料的語言不是該筆資料被蒐集時的語言，而當事人要求其個人資料必須以其被蒐集時的語言呈現，那麼如果個人願意支付翻譯的費用，該機構必須以其被蒐集時的語言回覆當事人。<br><br>（繼續） |

PRINCIPLES

**VIII. Access and orrection**

COMMENTARY

（continue）

23-25.

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

Where individual requests access to his or her information, that information should be provided in the language in which it is currently held. Where information is held in a language different to the language of original collection, and if the individual requests the information be provided in that original language, an organization should supply the information in the original language if the individual pays the cost of translation.

（continue）

| 原則 | 說明 |
| --- | --- |
| **VIII. 查閱和更正** | |
| | （繼續）<br>23-25.<br>請求查閱和更正個人資料的詳細程序可能會因為資料的特性或是其它利益考量而有所不同。因此，在某些情況下，變更、隱藏或刪除個人資料是不可能、不實際或沒有必要的。<br><br>為了與查閱的基本功能維持一致，機構應竭力地提供個人查閱個人資料。例如當某些資訊需要受到保護且當有人請求,查閱可以和該資訊分離提供的資訊時，那麼機構應將受到保護的資料保留下來，而將其它部分提供給個人查閱。但是，在某些情況機構有必要拒絕個人提出的查閱和更正請求，而此原則亦說明了在那些情況下機構可以拒絕個人的查閱和更正請求，包括查閱或更正的請求會造成機構不合理的負担或成本，例如個人重複提出相同的查閱或更正的請求或是該請求本質上是令人困擾的，當提供個人資料的查閱或更正會構成不法行為或對安全造成危害，或者為了保護機構的商業秘密，且該商業秘密一旦被揭露後將會有益於其他競爭者，例如特定的電腦或模組程式。<br><br>（繼續） |

PRINCIPLES

**VIII. Access and orrection**

COMMENTARY

（continue）

23-25.

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.

（continue）

| 原則 | 說明 |
| --- | --- |
| **VIII. 查閱和更正** | |
| | （繼續）<br>23-25.<br>商業秘密是指機構有採取防止措施防止被揭露的資訊，且一旦該資訊被揭露後，將為市場上競爭對手利用，造成機構財務上的損失。機構所利用的特定電腦程式或商業程序，例如模式程式，或是該程式或商業程序的細節可能是一種秘密性的商業資訊。當該秘密性商業資訊可以和其他資訊分離時，如果個人有提出查閱需求時，機構應將資訊分離，將構成個人資訊部分之非秘密性的商業資訊提供予個人查閱。當不可能將資料分離時且允許個人查閱會造成機構的商業秘密的洩露或是造成該機構對負有保密義務的另一家機構商業秘密的洩露，那麼機構可以限制或拒絕查閱請求。<br><br>當機構基於上列之理由而拒絕個人之查閱請求時，機構必須向個人說明其拒絕個人請求查閱的原因。但是，當允許個人查閱將會構成違法行為時，機構可以不提供說明。 |

| PRINCIPLES | COMMENTARY |
| --- | --- |
| **VIII. Access and orrection** | (continue)<br>23-25.<br>"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.<br><br>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, however, in cases where such disclosure would violate a law or judicial order. |

| 原則 | 說明 |
| --- | --- |
| **IX. 責任** | |
| 26. 個人資料管理者應要負責確保上列的原則之實踐。於傳遞個人資料於第三人時(不論是在國內或國外)，個人資料管理者應要取得個人的同意或必須竭力確保該第三人會採取和此一隱私保護綱領一致的措施以保護個人資訊隱私之安全。 | 26. 一個有效率且具有成本效率的商業經營模式通常需要於不同的機構間傳遞資訊。於傳遞資訊時，個人資料管理者必須採取合理的步驟確保個人資料於傳遞於第三人後，第三人仍會按本綱領所列的各項原則保護個人資料。但是，確實在某些狀況中，根本不可能或是難以確認第三人仍會按本綱領所列的各項原則保護個人資料，例如個人資料管理者和該第三人並沒任何關係。在這些情況中，個人資料管理者可以選擇其它方式，例如取得同意，以確保個人資料將會按隱私保護綱領中的各項原則受到保護。但是，如果個人資料的揭露是基於法律之要求，個人資料管理者則不需要取得同意，亦不需要採取任何措施確保第三人仍會按本綱領所列的各項原則保護個人資料。 |

| PRINCIPLES | COMMENTARY |
| --- | --- |
| **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 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. |

# 第四章. 執行

27. 第四章旨在提供會員經濟體有關於如何執行 APEC 隱私保護綱領的綱要。A 部分主要著重於會員經濟體於其境內該如何執行 APEC 隱私保護綱領時應考量的措施，而 B 部分則著重於會員經濟體該如何執行 APEC 隱私保護綱領中關於國際規範的部分。

## A. 境內執行綱要

### I. 追求隱私保護和資訊流通利益最大化

28. 經濟體於其境內執行 APEC 隱私保護綱領時，所採行的措施應要考量到下列的基本概念：

29. 體認到經濟體追求其人民之經濟和社會利益最大化的優點，個人資料的蒐集、持有、處理、利用、傳遞和揭露，應以可同時兼顧個人資訊隱私之保護和促進境內和跨境資訊流通的方式為之。

30. 因此，當會員經濟體於建立或檢視他們的隱私保護措施是否與 APEC 隱私保護綱領以及境內現有的隱私保護綱領一致時，應要採取一切合理及適當的步驟避免及移除任何不必要的資訊流通障礙。

### II. 實踐 APEC 隱私保護綱領

31. 實踐 APEC 隱私保護綱領以及保障個人隱私的方法有很多，包括立法、行政、產業自律或是綜合上列各種方法以促使 APEC 隱私保護綱領中所提列的各項權利得以被確保和行使。此外，會員經濟體應要建立一套得以提供其境內與隱私保護相關之資訊的機制。在實務的運作上，各會員經濟體應可以適其狀況彈性地執行此一隱私保護綱領，包括透過中央政府、多個機關的聯合執法、產業自律組織、或綜合上列各種方法執行此一保護綱領。

## 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. 如同於 31 段所提出的，各會員經濟體實行 APEC 隱私保護綱領的方式可能不同，而各經濟體對於 APEC 隱私保護綱領中的各項原則亦得以不同的方式執行之。不論所採取的執行方法為何，所有的目標都應要能夠在尊重各會員經濟體之需要下，使 APEC 地區之隱私保護途徑趨於一致。

33. APEC 經濟體對於在其境內發生的隱私侵害案件採取無差別的處理措施是值得鼓勵的。

34. 與境內的執法、國防、衛生及其他機構討論隱私保護綱領的執行，是確保 APEC 隱私保護之執行不與境內之國家安全、公共安全及其他公共政策任務相左的最佳途徑。

## III. 教育以及宣傳相關的隱私保護措施

35. 對於所有的會員經濟體，尤其是處於發展隱私保護方法初期之會員經濟體而言，APEC 隱私保護綱領希望可以提供他們一個參考方向。

36. 為了要施行 APEC 隱私保護綱領，此一隱私保護綱領應要廣為眾人所悉知。依此，各會員經濟體應要：

a) 宣傳其提供予個人的隱私保護措施；

b) 教育個人資料管理者關於會員經濟體之隱私保護措施；以及

c) 教育當事人其隱私受到侵害時的救濟途徑。

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. 公部門與私部間相互合作

37. 非政府部門的參與有助於 APEC 隱私保護綱領的實行。依此，各會員經濟體應與相關的私部門，包括隱私保護團體和消費者及產業代表就隱私保護之議題進行對話，以取得其意見並與其合作以促進 APEC 隱私保護綱領之目標的實踐。再者，各會員經濟體，尤其是尚未建立任何隱私保護機制的經濟體，應要注意在發展隱私保護的過程中私部門的意見是否有被反映出來。特別是各會員經濟體應要尋求和在公共教育方面與私部門合作的機會，鼓勵私部門對於隱私執行機構提出建議和批評以及鼓勵其和政府部門合作調查該些批評。

## V. 對於隱私侵害提供適當的救濟

38. 會員經濟體的隱私保護機制應對於隱私侵害提供適當的救濟，包括賠償、停止侵害以及其他救濟方法。在決定上列所稱的救濟範圍時，會員經濟體應考量下列幾點：

a) 會員經濟體所設計的隱私保護機制(例如執法單位的權力，這包括了個人可以提起訴訟的權利，產業自律規範或綜合上述所稱的各種機制)；和

b) 所提供的救濟應與個人之隱私受到侵害所造成的損害相當。

## VI. APEC 隱私保護綱領之境內執行報告機制

39. 各會員經濟體應要以完成及定期更新 Individual Action Plan (IAP)的方式公開其關於 APEC 隱私保護綱領的國內執行報告。

## 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.國際執行指南**

會員經濟體於重視 APEC 隱私權保護綱領之國際執行，以及其與 A 部分條文之一貫性時，應審酌下列與個人資料隱私保護有關之事項：

**Ⅰ會員經濟體相互間資訊分享**

40. 會員經濟體應盡力分享和交換對隱私保護有重大影響之資訊、調查與研究。

41. 為貫徹第 35 條及第 36 條之立法目的，會員經濟體應盡力就與隱私保護有關之問題相互施教，並分享與交換實施宣導、教育與訓練課程之資訊，俾喚起民眾意識，以及使社會大眾更加認識隱私保護和遵守相關法令之重要性。

42. 會員經濟體應盡力分享違反隱私保護案件之各種調查技術與經驗，以及因而產生之爭議解決指導策略，如申訴處理與訴訟外爭端解決機制。

43. 會員經濟體應指定其管轄權內負責履行相互間分享隱私保護相關資訊及執行跨國合作之主管機關，並通知其他會員經濟體。

**Ⅱ跨國調查與執行合作**

44. .建立合作架構：會員經濟體通盤考量現有國際合作架構與已有或現正研擬中之自我管控方案（包括以下 BⅢ部分所定者在內），且在內國法律與政策許可情況下，應審酌建立有助於跨國執行隱私權保護法律之合作機制與程序。此類合作架構得採取雙邊或多邊之模式。本項所定之跨國合作，會員經濟體遇有如遵守合作之要求，將牴觸內國法律、政策或優先事務，或資源匱乏或就繫爭之調查案件缺乏共同利益者，得婉拒或限制就特定請求調查案件或事項提供合作。

## 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. 關於隱私權保護法律之民事執行，跨國合作架構得包括下列事項：

(a) 能迅速、系統化及有效地將索定以某一會員經濟體內違法行為，或損及其人民權利之調查或隱私執行案件，通知該會員經濟體指定主管機關之機制。

(b) 有效分享重要資訊，使跨國合作調查隱私侵害與執行案件得以順利完成任務之機制。

(c) 針對隱私執行案件提供調查協助之機制。

(d) 以案件所涉違法侵害個人資料隱私之嚴重性與實際及可能導致之損害，以及其他相關因素，作為判定與其他會員經濟體指定之主管機關優先進行合作之機制。

(e) 依合作架構交換之資訊，使其能維持適當保密程度之措施。

### Ⅲ共同建立跨國隱私規章

46. 會員經濟體經認定企業定會負責遵守內國資料保護規定及其他相關法令者，將盡力支持該企業在亞太區域內建立跨國隱私規章，並加以承認或接受。此類跨國隱私規章，應遵守 APEC 隱私原則。

47. 會員經濟體將盡力與有切身利害關係者共同建立彼此相互承認或接受此類跨國隱私規章之架構或機制，以使其具法律效力。

48. 會員經濟體應確保此類跨國隱私規章及其承認或接受機制，能促進負責盡職地跨國資料傳遞，以及有效地隱私保護，而不致對跨國資訊流通造成不必要障礙，包括不對企業和消費者造成額外行政與官僚體系上之負擔。

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 crossborder 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.