編撰「個人隱私資料實務建議」，旨在提供公務單位報行個人隱私資料保護之參考。

個人隱私資料實務建議

◎盧玲朱

壹、緒論

鑒於個人隱私資料洩漏案件屢見不鮮，一般民眾之個人資料隨時可能透過網路購物或線上轉帳，藉由電腦漏洞、木馬或網路釣魚等方式，在不知不覺的狀況下外洩個人帳務資料。

- **案例一：**
  聯合報 97 年 08 月 27 日報導刑事局破獲兩岸駭客聯手入侵政府機關網站，盜取個人資料販賣牟利，包括現任總統、卸任總統和國安情治首長的個人資料，只要花 300 元，全都一覽無遺。警方說，查獲的資料庫多達五千多萬筆。

- **案例二：**
  中國時報 97 年 05 月 12 日報導智利一名電腦駭客從政府及軍方的伺服器中，盜走 600 萬人的機密資料，隨後即將所盜取之全部資料貼在一個科技論壇的部落格上。這些資料包括個人的身分證號碼、住址、電話號碼及學歷背景等。

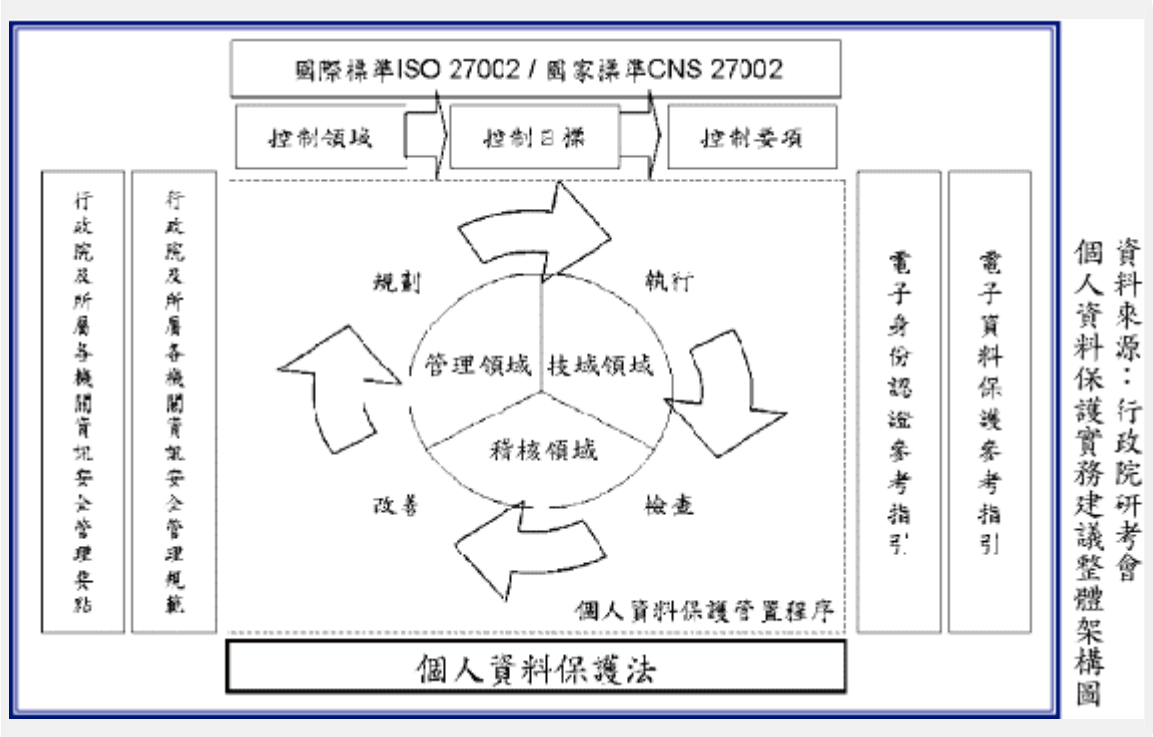
爲防範個人資料遭盜用或不當使用，以美國爲例，在 50 州中已有 44 州立法規定，發生個資外洩事件的機關(構)或企業，依法必須通報其客戶以減少損害。本文主要爲規劃我國個人資料保護的標準架構，以提供政府機關(構)整體管理程序之建議。

貳、個人隱私資料保護實務建議

行政院研考會爲有效因應個人隱私資料保護，於 97 年委託行政院國家資通安全會報技術服務中心編撰個人隱私資料保護實務建議（以下簡稱「實務建議」），作爲公務單位執行個人隱私資料保護之參考。

本實務建議參考我國資安標準、管理要點、管理規範以及國際標準「ISO 27002 資訊安全管理系統(Information Security Management System, ISMS)」之架構，提供個人隱私資料保護原則性的「實務建議」，內容訂定採規劃(Plan)、執行(Do)、檢查(Check)、改善(Act)之循環模式，及「控制領域(Domain)」、「控制目標(Objective)」、「控制要項(Control)」三層式執行架構編撰而成。

本實務建議整體架構如附圖所示：



王昭君的白玉雕塑

以下將針對實務建議之三項重點內容「個人資料保護管理程序」、「蒐集、處理與利用原則」以及「當事人之權利」詳予說明：

一、個人資料保護管理程序

個人隱私資料保護管理程序包括政策、機關、規劃、執行、檢查及改善措施；管理程序之目的爲保護機關爲其職務或業務而使用個人隱私資料時，能有效維護當事人資料之權益。不論任何機關，只要其營運行爲涉及個人資料的蒐集、處理、利用及國際傳輸，皆可適用。個人資料保護管理程序控制要項如下：

1. 確認個人資料保護管理程序與國家標準或規範一致，若目前並無相關標準及規範，機關可依據個資法之條文，制訂機關內之政策及指派執行人員。
2. 建立個人資料保護管理程序，即依據政策，規劃管理程序相關事項，包括指導方針、風險識別與分析、角色與權責、應變程序等。
3. 實作個人資料保護管理程序，即執行管理程序之運作程序、蒐集、處理與利用原則、適當之控制、當事人之權利、教育訓練及認證、資料加密技術、存取控制技術、流程管理技術及內部防禦技術。
4. 維護個人資料保護管理程序，即執行管理程序之檢查措施，含文件管制、員工的監督、受託人的監督、訴願及諮詢服務等。
5. 改進個人資料保護管理程序，即執行管理程序之稽核措施，含矯正與預防措施及管理階層的審查作業。

二、蒐集、處理與利用原則

蒐集、處理與利用原則之控制要項如下。

1. 機關應合法且適當地蒐集、處理個人資料。
2. 當機關蒐集、處理個人資料時，應限定利用目的，且應在達成目的所需必要範圍內蒐集、處理個人資料。

3. 個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實且信用之方法爲之，不得逾越特定目的之範圍（個資法修正草案第 5 條）。
4. 機關不應蒐集、處理或利用有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料（個資法修正草案第 6 條）。
5. 機關直接向當事人蒐集個人資料時，應明確告知當事人蒐集個人資料之目的、類別及利用方式（個資法修正草案第 8 條）。
6. 機關蒐集之個人資料非由當事人直接提供時，應具相關之告知措施（個資法修正草案第 9 條）。

三、當事人之權利

當事人權利之控制要項如下：

1. 對個人資料而言，機關有權責依當事人請求作回應（個資法修正草案第 3 條）。
2. 機關應將個人資料檔案名稱、機關的聯絡方式、類別及利用目的等事項公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同（個資法修正草案第 17 條）。
3. 當機關回應當事人時，應注意不要造成當事人負擔。
4. 機關應依當事人請求，就其蒐集之個人資料，執行查詢、閱覽或製給複製本予當事人（個資法修正草案第 10 條）。
5. 機關爲維護個人資料之正確，應依當事人之請求更正或補充之（個資法修正草案第 11 條第 1、5 項）。
6. 個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用（個資法修正草案第 11 條第 2、3、4 項）。
7. 個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除或停止利用該個人資料。
8. 違反法律規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除或停止利用該個人資料。

參、結語

上述「實務建議」主要係參考「日本 JIS Q 15001」的標準架構及我國「個人資料保護法修法草案」內容；技術領域控制目標主要參考研考會的「電子身分認證參考指引」及「電子資料保護參考指引」中相關於個人資料保護的技術建議，另外再補充資安內部防禦技術的建議而成。

機關(構)於使用本「實務建議」時，可結合內部之資通安全管理制度一併使用，配合檢討修訂與保護個人資料相關之政策、程序、規範及檢查表即可，不需重新訂定「個人隱私保護」之相關規定；亦可考量將個人隱私保護之業務合併於資通安全長(CISO)職務內，以期於政府有限資源內，發揮「個人隱私保護」之最大效益。

（作者任職國家資通安全會報技術服務中心）