公務機關執行個人資料保護法之參考事項

104.8.24

一、個人資料保護之規劃，包括下列事項：

（一）配置管理之人員及相當資源：

訂定個人資料保護管理相關規範，公告全體人員周知，以落實執行個人資料保護管理，並透過定期檢查、內評或檢視之方式，持續檢討修正之。

103 年政府機關（構）資通安全稽核相關建議參考事項：

1. 雖已訂定個資管理組織架構，惟相關管理人員之權責或配置之資源仍未明確。
2. 個人資料保護管理執行小組委員涵蓋範圍不足，例如：未納入人事及主計單位人員。
3. 個資管理制度，除參考其他已有完整個人資料管理制度之組織作法外，可依據本身規模與屬性進行調整。如個資作業流程控管、個資風險評鑑、個資內部稽核等工作，可考慮與內控制度適度整合，以降低人員負擔並提升控管有效性。
4. 宜依業務需求，研訂明確之作業流程分析及內部管理程序，以利於強化個資管理效果。

（二）個人資料盤點：

1、 清查各作業流程中所使用之表單、紀錄，並辨識個人資料有關之表單、紀錄，歸納整理為個人資料檔案。

2、 檢視保有之個人資料檔案，確認個人資料檔案名稱、保有依據、特定目的及個人資料類別。

3、 依個人資料保護法（下稱本法）第 17 條登載保有個人資料檔案公開項目。

4、 為維持個人資料檔案公開項目彙整表為最新之狀態，應定期檢視其更新狀況。

103 年政府機關（構）資通安全稽核相關建議參考事項：

1. 未明確訂定個資盤點作業時程，宜定期每年最少舉辦 1 次。
2. 個資盤點應配合業務作業流程訂定分工原則。
3. 個人資料以作業流程面向進行盤點，若過於複雜，可考量採流程圖方式繪製出個資生命週期，並呈現出相關利害關係者。

（三）個人資料之風險評估：

1、 就登載之個人資料檔案公開項目彙整表中之個人資料及各作業流程，分析可能產生之風險，並根據風險分析之結果，訂定適當之管控措施。

2、 為維持個人資料風險評估為最新之狀態，應定期檢視其更新狀況。

103 年政府機關（構）資通安全稽核相關建議參考事項：

1. 雖已進行個資盤點，但未定期進行後續之風險評估、衝擊分析及管理機制。
2. 風險評鑑方式應適切反應資安與個資風險。
3. 為定期進行個資風險評估、衝擊分析，建議能將所有個人資料周延納入，定期檢討分析，依不同個資類型或來源，予以檢視，俾充分發揮其功能。
4. 於個資風險評鑑中，宜訂定風險門檻值，以決定可接受之風險，後續每年應賡續滾動檢討。
5. 針對個資風險評估之結果，宜確認是否已採行適當之控制措施。

（四）事故之預防、通報及應變機制：

1、 依本法第18條及本法施行細則第12條採取技術上及組織上之措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

2、 建立事故通報機制，並採取適當之應變措施，以控制事故對當事人之損害。

3、 依本法第 12 條及本法施行細則第 22 條所定適當方式，通知當事人被侵害之事實及已採取之因應措施。

4、 查明事故之狀況，進行事故分析，研議預防機制，避免類似事故再次發生。

103 年政府機關（構）資通安全稽核相關建議參考事項：

1. 宜強化個人資料事故通報應變機制流程之完整性，包括通報之對象、時間、結案及檢討等面向。
2. 個人資料事故之預防、通報及緊急應變機制有所欠缺或未詳盡，宜訂定明確之處理流程或應變計畫，可參酌資安事件(故)的通報與緊急應變機制予以訂定或將其整併。

（五）認知宣導及教育訓練：

定期對於所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令之要求、所屬人員之責任範圍及各種個人資料保護事項之方法或管理措施。

103 年政府機關（構）資通安全稽核相關建議參考事項：

1. 進行個資風險評鑑及稽核作業前，建議增加相關教育訓練課程及輔導作業，俾利相關作業順利進行。
2. 所舉辦之個資宣導及資訊安全教育訓練，可加強其訓練成效，如意見交流及互動與回饋機制。

二、個人資料蒐集、處理及利用之管理程序，包括下列事項：

（一）依本法第 6 條之特種個人資料之屬性，分別訂定管理程序：

1、 檢視所蒐集、處理及利用之個人資料是否包含特種個人資料及其特定目的。

2、 檢視蒐集、處理及利用特種個人資料，是否符合相關法規之要件。如無特別規定，在本法第 6 條尚未施行前，仍適用本法第 15 條、第 16 條規定。

3、 雖非特種個人資料（例如：指紋、聲紋等資料），惟如認為具有特別管理之需要，仍得比照或訂定特別管理程序。

（二）為查知蒐集、處理及利用一般個人資料（非屬特種個人資料）行為，有無符合本法規定，宜採取下列方法：

1、 檢視蒐集、處理個人資料是否符合本法第 15 條規定，具有特定目的及法定要件。

2、 檢視利用個人資料是否符合本法第 16 條規定，符合特定目的內利用；於特定目的外利用個人資料時，應檢視是否具備法定特定目的外利用要件。

103 年政府機關（構）資通安全稽核相關建議參考事項：

1. 個資之蒐集、處理及利用過程，雖已設有專用表單進行管控，惟尚未研訂整體之管理程序與流程，無法瞭解各相關單位間之權責與分工作業，及個資利用之生命週期，供作嗣後政府公開資料之參考，宜研擬繪製管理流程圖。
2. 重點業務之個人資料檔案，若經常性提供予其他機關(構)介接或再利用，宜審慎評估適法性，妥適規劃資料提供之稽核管理機制，並促請再利用機關（構）注意資料使用及保管亦應符合本法規定。

（三）為遵守本法第 8 條及第 9 條關於告知義務之規定，應採取下列方法：

1、檢視蒐集、處理個人資料之特定目的。

2、檢視是否符合免告知之事由。

3、依據資料蒐集之情形，依本法施行細則第 16 條採取適當之告知方式。

（四）委託他人蒐集、處理或利用個人資料之全部或一部時，應對受託人依本法施行細則第 8 條規定為適當之監督，並明確約定相關監督事項與方式。

103 年政府機關（構）資通安全稽核相關建議參考事項：

1. 現行個人資料蒐集、處理或利用作業相關委外合約，除現有保密條款外，建議參考個資法施行細則第 8 條及第 12 條內容，強化受託廠商履行安全管理措施等責任。 2. 建議應明確訂定對委外廠商蒐集、處理及利用個人資料之稽核機制及作業流程圖，以落實委外廠商之監督作業。 3. 對委外廠商之個資稽核，建議於檢查表單列出廠商所持有個資之形式與內容，以及網站(系統)之帳號。

（五）當事人行使本法第 3 條所規定之權利時，非公務機關得採取下列方法為之：

1、確認是否為個人資料之本人。

2、提供當事人行使權利之方式，並遵守本法第 13 條有關處理期限之規定。

3、告知所酌收必要成本費用之標準。

4、如認有本法第 10 條及第 11 條得拒絕當事人行使權利之事由，一併附理由通知當事人。

（六）為維護其所保有個人資料之正確性，宜採取下列方法：

1、檢視個人資料於蒐集、處理或利用過程，是否正確。

2、當發現個人資料不正確時，應適時更正或補充；若該不正確可歸責於公務機關者，應通知曾提供利用之對象。

3、個人資料正確性有爭議者，依本法第 11 條第 2 項規定處理之方式。

（七）檢視其所保有個人資料之特定目的是否消失，或期限是否屆滿；確認特定目的消失或期限屆滿時，應依本法第 11 條第 3 項規定處理。

三、個人資料安全管理措施，包括下列事項：

（一）資料安全管理措施：

1、建立個人資料檔案分級分類管理制度，並針對接觸人員建立安全管理規範。

2、應針對資料存取、系統存取、網路存取等設定控制機制。

3、設定資料存取控制時，應考量業務性質及作業之必要，根據資料處理之方式設計之。必要時，考量採取權限區隔、資料加密機制或相關核准程序加以控管，並留存使用者身分，識別帳號與其行為紀錄，以供事後稽查。

4、針對所保有之個人資料內容，如有加密之需要，於蒐集、處理或利用時，宜採取適當之加密機制，例如於實體文件封袋上加上彌封或對資料檔案壓縮加密，並對轉交或傳輸行為加以記錄流向，以供備查。

5、作業過程有備份個人資料之需要時，應比照原件，依本法規定予以保護之。

6、個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物，嗣該媒介物於報廢或轉作其他用途時，宜採適當防範措施，以免由該媒介物洩漏個人資料。

103 年政府機關（構）資通安全稽核相關建議參考事項：

1. 有關個資儲存設備，如硬碟之報廢銷毀宜有更嚴謹之機制，不宜併同於其它產品處理清單內，交由廠商辦理。
2. 如使用回收紙裁切充當會議室之便條紙，應注意其背面有無個人資料；若有，則宜銷毀(塗銷)，不應再使用之。

（二）人員管理措施：

1、依據作業之需要，適度設定所屬人員不同之權限並控管其接觸個人資料之情形。

2、檢視各相關業務流程涉及蒐集、處理及利用個人資料之負責人員。

3、必要時得要求相關人員簽訂保密協定，約定保密義務。

（三）保有個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦或自動化機器設備等媒介物之環境，宜採取下列設備安全管理措施：

1、依據作業內容之不同，實施適宜之進出管制方式。

2、所屬人員應妥善保管個人資料之儲存媒介物。

3、針對不同媒介物存在之環境，審酌建置適度之保護設備或技術。

103 年政府機關（構）資通安全稽核相關建議參考事項：

建議強化個資檔案因業務需要存放於外網電腦之安全管理。

四、個人資料之安全稽核、紀錄保存及改善機制，包括下列事項：

(一) 為確保安全稽核及改善，宜建立個人資料安全稽核制度，定期查察機關個人資料檔案安全維護管理等相關事項。

103 年政府機關（構）資通安全稽核相關建議參考事項：

1. 個人資料安全稽核僅由各單位個人資料保護專責人員自行評估，則稽核結果無法確認，應儘速執行該單位之個人資料安全稽核。 2. 個人資料內部稽核後，應確認各單位矯正計畫或措施之有效性及時限。

3. 重點業務之個人資料檔案，若經常性提供予其他機關(構)介接或再利用，宜審慎評估適法性，妥適規劃資料提供之稽核管理機制，並促請再利用機關（構）注意資料使用及保管亦應符合本法規定。

(二) 採取個人資料使用紀錄、留存自動化機器設備之軌跡資料或其他相關證據保存機制，以供說明其執行個人資料檔案安全維護事項之情況。

103 年政府機關（構）資通安全稽核相關建議參考事項：

宜儘速建立個資查詢軌跡資料、安全維護、管理審查等管理措施。

(三) 為個人資料安全維護之整體持續改善，宜參酌執行業務現況、社會輿情、技術發展、法令變化等因素，注意下列事項：

1、檢視或修訂個人資料保護管理相關規範。

2、針對個人資料安全稽核結果有發現應糾正或改善事項者，宜規劃、執行改善及預防措施。

103 年政府機關（構）資通安全稽核相關建議參考事項：

1. 宜定期執行個人資料管理審查會議，確實維持個人資料安全管理之整體改善方案。
2. 建議將個人資料風險評鑑結果及內部評核結果之改善措施及執行情形，納入管理審查會議之討論議題，以確認其有效性定期管考。