中央目的事業主管機關依個人資料保護法第二十七條第三項規定訂定辦法之參考事項

一、 中央目的事業主管機關依個人資料保護法(下稱本法)第二十七條第二項規定指定非公務機關及依本法第二十七條第三項訂定計畫及處理方法之標準等相關事項之辦法，宜審酌非公務機關規模、特性、保有個人資料之性質及數量等事項，並參酌本法施行細則第十二條規定之適當安全措施事項定之。

非公務機關依本法第二十七條第三項訂定計畫及處理方法之標準等相關事項之辦法，得包括本參考事項第二點至第五點，並參酌前項事項，酌予調整。

二、 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：

1、 規劃、訂定、修正與執行個人資料檔案安全維護計畫或業務終止後個人資料處理方法等相關事項，並定期向所屬非公務機關提出報告。

2、 訂定個人資料保護管理政策，將其所蒐集、處理及利用個人資料之依據、特定目的及其他相關保護事項，公告使其所屬人員均明確瞭解。

(二)界定個人資料之範圍：

1、 定期清查保有之個人資料現況。

2、 確認保有之個人資料所應遵循適用之個人資料保護相關法令現況。

(三)個人資料之風險評估及管理機制：依已界定之個人資料範圍及個人資料蒐集、處理、利用之流程，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。

(四)為因應所保有之個人資料被竊取、竄改、毀損、滅失或洩漏等事故之預防、通報及應變機制：

1、 採取適當之應變措施，以控制事故對當事人之損害，並通報有關單位。

2、 查明事故之狀況並以適當方式通知當事人。

3、 研議預防機制，避免類似事故再次發生。

(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。

三、 個人資料之管理程序，包括下列事項：

(一)依一般個人資料及本法第六條之特種個人資料之屬性，分別訂定下列管理程序：

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，是否符合相關法令之要件。

3、 雖非特種個人資料，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)為遵守本法第八條及第九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。

(三)為查知蒐集、處理及利用一般個人資料行為，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十九條規定，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二十條第一項規定，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。

(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八條規定為適當之監督，並明確約定相關監督事項與方式。

(五)利用個人資料為行銷時，應檢視下列事項：

1、 當事人表示拒絕行銷後，應立即停止利用其個人資料行銷，並週知所屬人員。

2、 至少於首次行銷時，提供當事人免費表示拒絕接受行銷之方式。

(六)進行個人資料國際傳輸前，檢視有無中央目的事業主管機關依本法第二十一條規定為限制國際傳輸之命令或處分，並應遵循之。

(七)當事人行使本法第三條所規定之權利時，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，並遵守本法第十三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、 如認有本法第十條及第十一條得拒絕當事人行使權利之事由，一併附理由通知當事人。

(八)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非公務機關者，應通知曾提供利用之對象。

3、 個人資料正確性有爭議者，依本法第十一條第二項規定處理之方式。

(九)非公務機關應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，應依本法第十一條第三項規定處理。

四、 個人資料之管理措施，包括下列事項：

(一)資料安全管理措施：

1、 運用電腦或自動化機器相關設備蒐集、處理或利用個人資料時，宜訂定使用可攜式設備或儲存媒體之規範。

2、 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。

3、 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。

4、 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；若委託他人執行上開行為時，宜依本參考事項第三點第四款規定辦理。

(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、 與所屬人員約定保密義務。

(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。

(四)業務終止後個人資料處理方法得參酌下列方式為之，並留存下列紀錄：

1、 銷毀：銷毀之方法、時間、地點及證明銷毀之方式。

2、 移轉：移轉之原因、對象、方法、時間、地點及受移轉對象

得保有該項個人資料之合法依據。

3、 其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。

五、 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，宜採取個人資料安全稽核機制，查察該機關是否落實其所訂定之個人資料檔案安全維護計畫或業務終止後個人資料處理方法等相關事項，以符合法令規範。

(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，以供說明其執行所訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法等相關個人資料保護事項之情況。

(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檔案安全維護計畫或業務終止後個人資料處理方法等相關個人資料保護事項。

2、 針對個人資料安全稽核結果之不符合法令之虞者，宜規劃、執行改善及預防措施。