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草案總說明

法務部為協助各中央目的事業主管機關依個人資料保護法第 27 條第 3 項規定，訂定非公務機關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之標準等相關個人資料保護事項之辦法，爰研擬本參考事項草案初稿，於 101 年 5 月 11 日及 101 年 9 月 14 日召開會議邀集各機關進行討論並提供意見。經參考上開各機關所提意見，復參酌 P-D-C-A（Plan-Do-Check-Act）方法論後，爰擬具本參考事項，其重點如次：

一、 個人資料保護事項之規劃：

有關人員、資源、界定個人資料範圍、風險評估、通報應變措施、認知宣導及教育訓練等機制之規劃事項。（第二點）

二、 個人資料蒐集、處理及利用之管理程序：

有關蒐集、處理及利用個人資料時，宜採取之方法。（第三點）

三、 個人資料管理措施：

有關資料安全管理、人員管理、設備安全管理及業務終止後個人資料處理方法等事項。（第四點）

四、 個人資料安全稽核、紀錄保存及改善機制：

有關資料安全稽核機制、證據保存及整體持續改善事項。（第五點）

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

參考事項	說明
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。	一、中央目的事業主管機關得審酌指定非公務機關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辦法，以及訂定上開計畫及處理方法之標準。其指定及訂定時，除本法施行細則第十二條規定之適當安全措施事項，宜審酌下列事項： （一）非公務機關規模、特性：由於非公務機關之組織規模大小與事業特性不一，為使各中央目的事業主管機關所訂定之辦法能符合其實際需要，中央目的事業主管機關宜根據受指定非公務機關之組織規模大小與事業特性，依比例原則，衡酌所欲達成之個人資料保護目的，並參酌本法施行細則第十二條第二項所列技術上及組織上等適當安全維護措施事項，訂定不同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之標準等相關個人資料保護事項之辦法。 （二）非公務機關保有個人資料之性質及數量：鑑於部分行業保有大量且重要之個人資料檔案，宜加強其保護個人資料之安全維護措施。因此，中央目

	的事業主管機關得指定非公務機關(例如以行業別或其他條件限制下之非公務機關)，要求其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，以加強管理，確保個人資料之安全維護。 二、 非公務機關所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，應符合中央目的事業主管機關所定上開計畫或處理方法之標準等相關個人資料保護事項之辦法，並得參酌第一項所列相關事項，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	一、為有效訂定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個人資料保護事項，應配置適當之管理人員及資源，且該管理人員宜就上開事項，作相關程序之策劃、訂定、執行與修訂，並宜定期向所屬非公務機關報告上開事項之推動情形，爰為第一款第一目規定。 二、為使非公務機關全體人員對於個人資料之保護能有所體認，進而落實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，故非公務機關宜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於政策內闡明。且為達上述目的，該等政策宜予公告使其所屬人員均明確瞭解，爰為第

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。	一款第二目規定。 三、為瞭解其所蒐集、處理及利用之個人資料,宜先掌握其保有個人資料之內涵(例如:個人資料檔案名稱、個人資料類別等),以便有效規劃個人資料保護事項。另為瞭解其所蒐集、處理及利用之個人資料是否合法,宜清查所適用個人資料保護之關法令之現況(例如有無修正廢止),爰為第二款規定。 四、於界定個人資料之範圍後,宜參照其相關業務流程,判斷其於蒐集、處理及利用個人資料之過程中,可能發生非公務機關違反本法規定,致使個人資料被竊取、洩漏、竄改或其他侵害等事故,包含該等事故發生之原因、程度及頻率,方能進一步以適當管控措施保護個人資料並降低其風險,爰為第三款規定。 五、當非公務機關違反本法規定,致使個人資料被竊取、洩漏、竄改或其他侵害等事故發生時,常造成當事人財產及非財產上之損害,故為降低或控制損害之範圍,非公務機關應訂定相關之因應措施。另通知當事人之內容應包括個人資料被侵害之事實及已採取之因應措施(本法施行細則第二十二條第二項參照),爰為第四款規定。 六、為使非公務機關之所屬人員均能明瞭個人資料保護相關法令之要求、各該所屬人員之責任範圍及各種作業程序,故應透過定期舉辦基礎認知宣導及專業教育訓練為之,爰為第五款規定。

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	一、本法第六條雖尚未施行，惟因該條所定特種個人資料性較為特殊或具敏感性，故非公務機關宜注意是否有蒐集、處理及利用特種個人資料。另雖非特種資料，如有特別管理之需要者(例如：指紋、聲紋等個人資料)，亦得比照特種個人資料予以保護，爰為第一款規定。 二、依本法第八條及第九條規定，非公務機關原則上應適時履行告知義務，除經檢視有例外無須告知之事由外，依據資料蒐集之情形，採取適當之告知方式，以確實履行告知義務。所稱適當方式通知當事人，係指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之(本法施行細則第十六條規定參照)，爰為第二款規定。 三、為查知一般蒐集、處理、利用個人資料行為，有無符合本法第十九條及第二十條規定，爰為第三款規定。 四、非公務機關如將個人資料之蒐集、處理或利用委託他人為之，應對受託人為適當之監督，以使資料之蒐集、處理或利用仍符合法令之要求，爰為第四款規定。 五、為查知利用個人資料行銷行為，有無符合本法第二十條第二項及第三項規定，爰為第五款規定。 六、依本法第二十一條規定，中央目的事業主管機關得於一定情形下，限制非公務機關對於個人資料進行國際傳輸，因此非公務機關宜檢視上開主管機關是否有所限制，並予以遵守，爰為第六款規定。 七、非公務機關宜採取相關方法協助當

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	事人行使本法第三條、第十條及第十一條規定規定之權利，因此非公務機關宜檢視上開法令規定，並予以遵守，爰為第七款規定。 八、非公務機關所保有個人資料之正確性，攸關非公務機關是否能有效利用個人資料以提供當事人相關服務，並避免當事人遭受因資料不正確而生之損害。因此，非公務機關宜採取相關方法，檢視個人資料之正確性，爰為第八款規定。 九、蒐集、處理或利用個人資料，均應於特定目的必要範圍內為之，若蒐集、處理、利用個人資料之特定目的已消失或期限已屆滿，依本法第十一條第三項之規定，應予以刪除、停止處理或利用，爰為第九款規定。

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	一、使用可攜式設備或儲存媒體(指可攜帶且具備運算處理或資料擷取儲存功能之設備，例如：筆記型電腦、行動電話、隨身碟、記憶卡、光碟等)，可能提高個人資料外洩之風險，因此若有使用可攜式設備或儲存媒體之情況，宜訂定相關使用規範，爰為第一款第一目規定。 二、針對個人資料蒐集、處理及利用之不同態樣，如個人資料內容有加密之需要，即應採取適當之加密機

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。	制，爰為第一款第二目規定。 三、參照國家機保護法第十八條有關複製物與原件規定之立法例，非公務機關相關作業過程，有備份個人資料之需要時，應比照原件個人資料，採取適當之保護措施，爰為第一款第三目規定。 五、儲存個人資料之媒介物(參考政府資訊公開法第三條規定之立法例)，嗣報廢或轉作其他用途時(例如：移轉與他人)，宜採適當防範措施，以免由該媒介物洩漏個人資料(例如:燒毀、裁碎、磁性媒體予以消磁或破壞、回收再利用之紙本不含個人資料之記載部分等)。另倘委託第三者執行報廢或轉作其他用途時，宜依本參考事項第三點第四款規定辦理，爰為本點第一款第四目規定。 六、非公務機關就其保有之個人資料，宜對其所屬人員採取適當之監督措施，爰為第二款規定。 七、非公務機關就保有個人資料所存在之媒介物環境，宜採取適當之管理措施，爰為第三款規定。 八、為明定非公務機關於業務終止後，其陳報個人資料處理方法之應記載事項，爰為第四款規定。

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	非公務機關宜採取個人資料稽核(例如以複查或抽查方式等)、適當之證據保存及持續改善個人資料保護等機制，以落實執行個人資料保護相關事項。

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。	