

國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法

條 文	說 明
第一條 本辦法依個人資料保護法(以下簡稱本法)第二十七條第三項規定訂定之。	揭示本辦法之訂定依據。
第二條 本辦法所稱非公務機關包括下列各款： 一、第一類電信事業。 二、第二類電信事業。 三、有線廣播電視系統經營者及有線電視節目播送系統。 四、電視事業。 五、訂戶數達三千戶以上之直播衛星廣播電視服務事業。 六、經營國內新聞台頻道或購物頻道之衛星或他類頻道節目供應事業。	一、明定本辦法之適用範圍，包括依電信法、廣播電視法、有線廣播電視法或衛星廣播電視法取得許可或執照之非公務機關。 二、按法務部「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」第一點規定，中央目的事業主管機關依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規定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。依上開意旨，鑒於電信法第十一條第二項及第四項規定之第一、二類電信事業於行動寬頻網路及網際網路平臺之資料運用，或於傳輸平臺上之通訊資料傳遞，其特性與影響，皆與消費大眾之個人資料息息相關；且電信事業依電信法第六條第二項規定，負有保障通信秘密之義務，故均應適用本辦法之規定，爰訂定第一款及二款。 三、有線廣播電視法第二條第三款規定之有線廣播電視系統經營者及同法第七十三條規定之有線電視節目播送系統係屬系統或平臺，為提供其服務與帳務處理等事宜，於實務上有蒐集、處理及利用用戶之個人資料，應適用本辦法之規定，爰訂定第三款。 四、廣播電視法第二條第四款規定之電視事業雖提供免費收視(聽)(Free to Air)，無須蒐集、處理及利用用戶之個人資料，惟其於播報新聞時可能對被播報對象涉及申訴、更正與答辯等情事，而有蒐集個人資料之情形，應適用本辦法之規定，爰訂定第四款。 五、目前經營直播衛星廣播電視服務事業計有六家(境內兩家、境外四家)，雖

	屬系統，惟總體而言其經營規模小，總訂戶約計三萬戶，且主要訂戶為旅店業或飯店業者，非屬自然人，不適用個資法，然考量業者仍有蒐集個人資料之行為，故將規管範圍限縮為訂戶達三千戶以上者，爰訂定第五款。 六、衛星頻道節目供應事業及他類頻道節目供應事業，係屬頻道經營者，其提供節目於平臺播送且未與視聽眾訂定服務契約，未蒐集、處理及利用視聽眾之個人資料，原則上不納入本辦法之規範；惟其經營國內新聞台頻道或購物頻道，雖未與視聽眾訂定服務契約，但於實務經驗，其於播報新聞時可能對被播報對象涉及申訴、更正與答辯等情事，而有蒐集個人資料之情形，又經營購物頻道業者係以提供銷售資訊為主要經營內容，因涉及客服業務而衍生蒐集個人資料之行為，應適用本辦法之規定，爰訂定第六款。
第三條 非公務機關應依其業務規模及特性，衡酌經營資源之合理分配，配置管理之人員及相當資源，以規劃、訂定、修正與執行其個人資料檔案安全維護計畫及業務終止後個人資料處理方法(以下簡稱本計畫及處理方法)。 本計畫及處理方法之訂定或修正，應經非公務機關負責人或法定代理人簽署。 非公務機關蒐集、處理及利用達五千名用戶之個人資料者，其訂定之本計畫及處理方法內容應包含國內或國際個人資料安全稽核機制之規劃及執行計畫。	一、配合本法施行細則第十二條第二項第一款規定，非公務機關為落實個人資料保護目的，應考量組織規模與保有個人資料之數量或內容，依比例原則建立技術上及組織上之措施，俾規劃、訂定、修正與執行本計畫及處理方法之相關事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 二、又非公務機關針對用戶個人資料蒐集、處理及利用，均應考量技術演進及匯流發展所延伸之通訊傳播服務範圍，並據以規劃、訂定、修正與執行本計畫及處理方法之相關事項。 三、關於本計畫及處理方法之訂定或修正，是否須經非公務機關之負責人或法定代理人簽署，本法及本法施行細則未有明文，爰於本條第二項明定之，以利遵循。 四、日本「個人情報保護法」之規定對於資料庫於半年內之任何一日均未累積超過五千名特定個人資料之事業，不適用之；美國「消費者隱私保護法草案」(Consumer Privacy Protection Act of 2011, H.R.1528)於西元二零一一年四月十三日送交國會進行審

	議，草案中據以要求任何業者(covered entity)，只要在連續十二個月的期間內，有蒐集、販賣、有償公開或使用超過五千名消費者之個人資料者。因此，鑒於本法第二條第四款「處理」之定義，並參採日本與美國西元二零一一年「消費者隱私保護法草案」之處理筆數，爰於第三項明定，蒐集、處理及利用達五千名用戶個人資料之非公務機關，其訂定之本計畫及處理方法內容應包含國內(TPIPAS)或國際(P-Mark、ePrivacy-Mark、BS 等)個人資料安全稽核機制之規劃與執行計畫。 五、按本法第二十七條及本法施行細則第十二條第一項、第二項及其第九款之規定，應採行適當之安全措施及具有適當比例為原則，並對於資料安全施行稽核機制，爰參照本會主管之各項業務管理規則，目前業已增修資通安全管理專章，故本項條文，考量本會監理事業持有用戶之個人資料，具有業務特殊性及商業價值(可利用於行動商務小額付款平臺、網購服務及商業訊息播送上)，且非公務機關蒐集、處理及利用之個人資料達一定數量者，採<u>第三方</u>稽核機制。
第四條 非公務機關為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故(以下簡稱事故)，應訂定下列應變、通報及改善機制： 一、事故發生後應採取之應變措施，包括控制當事人損害之方式、查明事故後通知當事人之適當方式及內容。 二、事故發生後應受通報之對象及其通報方式。 三、事故發生後，其改善措施之研議機制。 非公務機關遇有重大個人資料事故者，應即通報國家通訊傳播委員會(以下簡稱本會)。 前項所稱重大個人資料事故，係指個人資料遭竊取、竄改、毀損、滅失或洩漏，將危及非公務機關正常營運或大	一、配合本法施行細則第十二條第二項第四款規定，明定應於本計畫及處理方法中訂定之個人資料安全事故應變、通報及改善機制。 二、按事故應變之首要目標，係根據事故之類型，採取應變措施降低或控制當事人損害之範圍，並儘速依本法第十二條、本法施行細則第二十二條等規定通知當事人。爰於第一款規定本計畫及處理方法之應變措施，應包括控制當事人損害之方式、查明事故後通知當事人之適當方式及內容。 三、次按行政院一百零四年二月十日召開「消費者個資外洩事件處理機制」研商會議決議，非公務機關如發生個人資料遭竊、外洩等事故，為使有關機關、單位及時掌握情況，自應以適當方式通報。為利執行，宜將此等通報

量當事人權益之情形。	對象及通報方式，一併明定於本計畫及處理辦法中，爰為第二款規定。 四、再按避免類似事故重複發生，亦為應變措施之重點，爰於第一項第三款規定本計畫及處理方法，應明定事故發生後改善措施之研議機制。 五、未按非公務機關如遭遇重大個人資料事故而危及其正常營運或多數當事人權益，應採取較一般事故更嚴密之應變及預防措施，爰於第二項明定應通報本會。
第五條 非公務機關應就下列事項，訂定個人資料之管理程序： 一、蒐集、處理或利用之個人資料包含本法第六條所定特種個人資料者，檢視其特定目的及是否符合相關法令之要件。 二、檢視個人資料之蒐集、處理或利用，是否符合免為告知之事由，及告知之內容、方式是否合法妥適。 三、檢視個人資料之蒐集、處理，是否符合本法第十九條規定，具有特定目的及法定情形；其經當事人同意者，並應確保符合本法第七條第一項規定。 四、檢視個人資料之利用，是否符合蒐集之特定目的必要範圍；其為特定目的外之利用者，檢視是否符合法定情形，經當事人同意者，並應確保符合本法第七條第二項規定。 五、利用個人資料為行銷，當事人表示拒絕行銷者，立即停止利用其個人資料行銷，並至少於首次行銷時，提供當事人免費表示拒絕接受行銷之方式。 六、委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人依本法施行細則第八條規定為適當之監督，並於委託契約或相關文件中，明確約定其內容。 七、進行個人資料國際傳輸前，檢視是否受本會相關法令限制並遵循之。 八、當事人行使本法第三條所定權利之相關事項： (一)當事人身分之確認。	一、配合本法施行細則第十二條第二項第五款規定，明定非公務機關應依本辦法將其個人資料蒐集、處理及利用之內部管理程序，明定於本計畫及處理方法中，包括：檢視一般或特種個人資料之蒐集、處理或利用是否符合法定要件；當事人拒絕行銷之處置；對受託人之監督事項；遵守本會所為國際傳輸之限制；當事人行使權利之處理；個人資料正確性之維護；個人資料之刪除等事項。 二、本條第二款告知義務之履行，非公務機關應確保相關告知事項符合本法第八條規定明確性之要求（例如：個人資料之類別，應具體說明所蒐集資料之類別：基本資料、通信資訊、位置資訊、瀏覽紀錄或收視紀錄等）；此外，告知內容並應儘可能使用淺顯易懂之文字，俾使當事人容易明瞭。 三、為符合本法第五條規定所揭櫫誠信原則與禁止不當聯結之意旨，非公務機關取得本條第三款及第四款當事人同意時，不得採取「網綁式同意」（例如：以定型化契約網綁與履行電信服務契約必要範圍無涉之行銷，若當事人拒絕同意，即不提供電信服務等）。又非公務機關應避免採取「預設同意」（使當事人須另為不同意之意思表示以拒絕同意）之方式以取得當事人同意。

(二)提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項。 (三)對當事人請求之審查方式，並遵守本法有關處理期限之規定。 (四)有本法所定得拒絕當事人行使權利之事由者，其理由記載及通知當事人之方式。 九、檢視個人資料於蒐集、處理或利用過程中是否正確；其有不正確或正確性有爭議者，應依本法第十一條第一項、第二項及第五項規定辦理。 十、檢視所保有個人資料之特定目的是否消失，或期限是否屆滿；其特定目的消失或期限屆滿者，應依本法第十一條第三項規定辦理。 十一、設置聯絡窗口供當事人申訴與諮詢。	
第六條 非公務機關應就下列事項，訂定相關紀錄、證據保存機制： 一、因執行本計畫及處理方法所定各種個人資料保護機制、程序及措施，所記錄之個人資料使用情況、軌跡資料及相關證據。 二、依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後留存之下列紀錄： (一)刪除、停止處理或利用之方法、時間。 (二)將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。	一、非公務機關為證明已落實本計畫及處理方法所定之機制、程序及措施，並釐清個人資料於蒐集、處理或利用過程之相關權責，應就個人資料使用情況、軌跡資料等建立保存機制。爰配合本法施行細則第十二條第二項第十款規定，於第一款明定非公務機關應於本計畫及處理方法中，訂定相關紀錄、證據保存機制。 二、非公務機關業務終止後，亦即特定目的消失或期限屆滿後，原則上應依本法第十一條第三項規定刪除、停止處理或利用相關個人資料；惟其是否實際刪除、停止處理或利用，當事人往往無從得知。為預防不必要之紛爭，爰於第二款明定非公務機關刪除、停止處理或利用所保有之個人資料後，應留存相關紀錄。又非公務機關雖將所保有之個人資料刪除，仍可能於刪除前將其備份資料移轉他人，爰於本款第二目併予規定應有合法依據，以求周延。
第七條 本辦法自發布日施行。	明定本辦法之施行日期。