通傳產業
個人資料保護與管理
實作指引手冊

通傳產業
個人資料保護與管理
實作指引手冊

目錄 CONTENTS

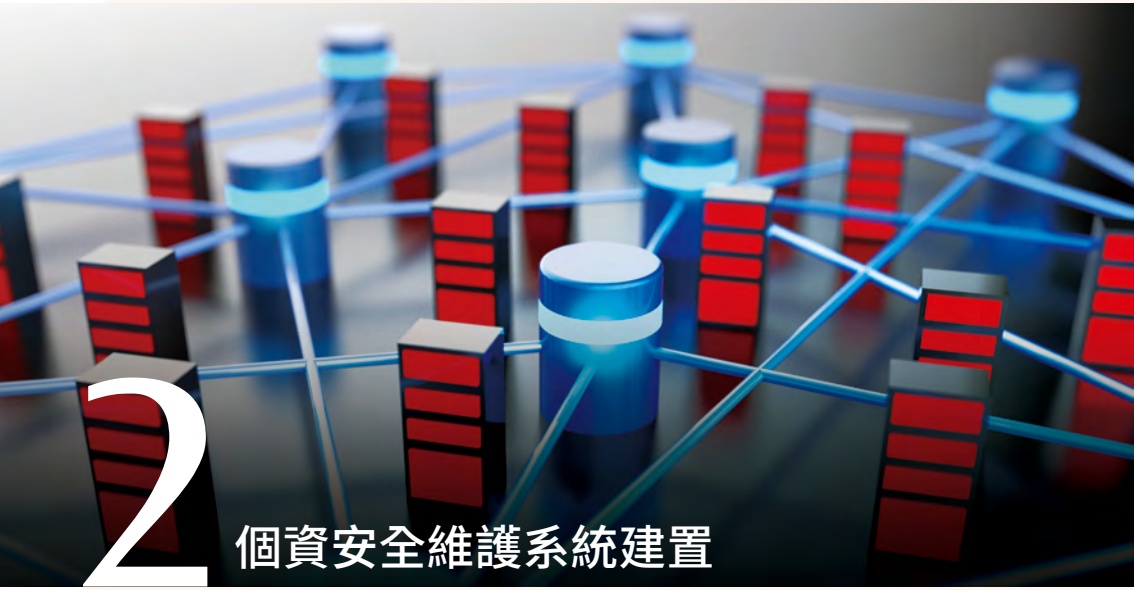
1 前言

數位時代來臨，全球產業經營型態產生新興科技模式，透過巨量資料之利用與剖析，成為數位經濟不可或缺的成功要素，更為現代新興商業模式營運之重要基礎。是以，近年來個資隱私保護與合法利用加值資料等議題備受關注。

由於通傳產業通常會掌握大量用戶的個人資料，而且個人資料保護法（簡稱個資法）與個人資料保護法施行細則（簡稱個資法施行細則）都明確規定，非公務機關單位如果保有個人資料檔案，應該要採取適當的安全維護措施。因此，國家通訊傳播委員於2016年11月發布「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」（簡稱安全維護辦法），讓通訊傳播事業單位在落實個人資料之保護及管理上有所依循，以促進企業組織內部落實個資法遵。

為了落實個人資料的安全維護，傳通業者應該建置公司內部的個人資料檔案安全維護程序及業務終止後個人資料處理機制。但是，實際上應該要怎麼做呢？所謂的管理計畫，應該包含哪些項目？個人資料安全維護事項有哪些？如何配置人力與資源？如何盤點個資？如何進行風險評估？公司內部資料安全維護規定的訂定、個資保護認知宣導及教育訓練、稽核與持續改善又都應該要如何進行？而個資的蒐集使用目的消失後或期限屆滿時，個人資料檔案該如何處理？

本手冊旨在針對通傳產業實務操作者提供個資管理的實務指引。將從個資保護與管理制度整體建置方法著手，納入執行個人資料保護管理時應注意的事項，並透過實際個資輔導訪查案例說明分析，使讀者更能清楚掌握個資保護管理實務之要點。



2 個資安全維護系統建置

一、個資安全維護措施

通傳產業根據產業特性從實務上來看，往往會因為特定目的而需要蒐集使用並保存個資，而我國個人資料保護法針對一般企業組織保存個資的情況，要求企業組織執行「適當安全維護措施」，防止個人資料被竊取、竄改、毀損、滅失或洩漏的情況發生。

什麼是「適當安全維護措施」呢？適當安全維護措施應該包含以下事項：

- 配置管理之人員及相當資源。
- 界定個人資料之範圍。
- 個人資料之風險評估及管理機制。

・事故之預防、通報及應變機制。

・個人資料蒐集、處理及利用之內部管理程序。

・資料安全管理及人員管理。

・認知宣導及教育訓練。

・設備安全管理。

・資料安全稽核機制。

・使用紀錄、軌跡資料及證據保存。

・個人資料安全維護之整體持續改善。

為了協助通傳產業業者有效建立「適當安全維護措施」，通訊傳播委員會公佈的安全維護辦法提供業者相當的指示及依循。然而，要更進一步的在企業體制內落實個人資料安全維護系統的建置及運作，應該要先明白個人資料安全維護之運作方法。

個資法小法典 個資法施行細則第12條

二、個資安全維護系統設計概念

我國個人資料保護相關法令與國內外個人資料管理系統[1]，皆以PDCA品質管理循環方法論作為管理系統設計基礎。所謂PDCA，是以Plan計畫→Do執行→Check檢查→Act行動為循環基礎之方法論。

1.計畫：制定規劃個人資料保護管理政策、目標及相關程序。

2.執行：落實個人資料管理制度。

3.檢查：依據個人資料保護管理政策、目標及要求，評估監督流程並檢視執行成果，將結果回報給最高管理階層加以審查。

4.行動：根據檢查結果採取措施，持續改善個人資料管理制度。

隨著計劃制定、計畫執行、執行檢查、採取改善措施等步驟持續循環，個人資料安全維護系統將會越趨完善整密。

▶實務操作提醒◀

個資保護缺一不可 PDCA循環精進

個人資料安全維護運作需透過PDCA不斷循環，除了計畫與執行個人資料保護與管理制度之建置，更需要透過組織內部稽核或外部審查，進而發現個資管理制度之缺失，加以矯正改善。

實務上許多組織只依個資法形式上建置管理制度，並未根本落實、實踐個人資料保護相關措施，亦未定期稽核個人資料保護制度，更遑論矯正改善。這樣的形式操作狀況下，導致組織潛在管理弱點未能被發現，個人資料保護與管理制度視同虛設，可能造成外部侵害破口與重大損害。

▶個資法遵建議◀

一年一循環 安全自然來

個人資料保護與管理制度至少應於每年循環檢視一次，進而確保組織內部個資保護管理機制為有效且符合組織現況。除此之外，當組織架構有重大變更或組織業務拓展時，應同步檢視個資保護管理制度或相關程序有無需要調整之處。

1 時下常見個人資料管理系統（Personal Information Management System, PIMS）例如臺灣個人資料保護與管理制度（TPIPAS）、BS10012、CNS29100等。

3 Plan—規劃與建置

建立個人資料安全維護系統及落實個人資料安全維護措施會涉及：組織投入的資源人力、個人資料蒐集處理利用的流程、個人資料檔案盤點及風險評估方法、事故應變處理程序、通報及改善機制、個人資料安全管理方法、當事人權利行使處理程序、委外監督、認知宣導及教育訓練、資訊安全稽核、使用紀錄及相關證據保存，以及持續改善措施等事項。

接下來將針對建置個人資料安全維護系統所涉及的各個事項逐一說明。

一、個人資料安全維護系統建置第一步驟：配置適當的管理人員及資源

組織必須要有一定的人力和資源投入，才能夠進行內部個資盤點與風險分析，也才有能力進一步規劃並執行事故應變、通報及改善機制、個人資料安全管理、當事人權利行使、委外監督等事項。

「配置管理人力」意思是，組織內部應透過專任或兼任方式指派專責人員承擔內部個人資料保護的責任，且所負責的個人資料安全維護工作屬於經常性業務。

需特別注意的是，我國與歐盟一般資料保護規則（General Data Protection Regulation, GDPR）對於專責人員的要求規範不同。我國的個資相關規範並沒有要求組織必須成立專職個人資料保護與管理的資料保護專員或個資長，只需要有專責人員負責組織內部個人資料保護即可。

配置「相當資源」的意思，是指組織提供維護及管理個人資料檔案所需要的資源，包括經費、技術支持等。以落實資料保護角度來說，組織若要確實做好個人資料安全維護，所投入的資源與人力應和組織規模成相當比例，否則可能會成效不彰。

▶實務操作提醒◀

- 實務上在規模較大的組織，若只有指派少數人進行個資安全維護工作，勢必會有所不足。因此，若能以建立「個資檔案安全維護管理小組」方式進行，並配合適當的認知宣導與教育訓練，才能有效落實適當安全維護措施。
- 建立個資管理小組，應該同時要考慮層級、功能、及業務性質等因素。管理小組的領導者，最好在單位內具有相當高度或管理權限，才能避免發生管理小組政策難以推動之窘況。
- 一定規模的組織，應該建立具備管理代表、執行人員與內評人員（詳見下圖）的個資管理小組。

1. 管理代表：組織個資管理制度之主要負責人，作為統籌整個管理組織並分配相關工作的角色。管理代表需定期向企業組織負責人報告，組織內部個資管理小組運作之相關事項。通常由企業最高管理階層指派一位總

經理或副總經理的管理階層，擔當組織內部個人資料保護之責任，並視推行情況提供執行監督人員必要的資源與協助。

2.管理人員：相較於管理代表負責統籌組織，決定政策，給予相關資源，管理人員為實際第一線執行之人員。為了有效推動企業組織個資管理制度，需因應企業規模與組織架構，各個部門應至少推派一名個資管理負責人員，負責辦理業務範圍內個資安全維護事項的經常性工作，例如該部門個資盤點、確認個人資料安全維護事項遵循狀況、個人資料安全維護事項落實等。

3.內評人員：為有效督導與評核個資保護管理程序運作及安全措施執行之成效，除個人資料管理代表外，管理組織亦應安排內部監督或評量計畫是否確實執行之監督人員。

這樣的管理結構有助於實質並有效地落實個資保護。如果遇到組織規模較小或組織人力與資源有限的情形，則管理與維護個人資料檔案的專責人員，可以由組織內部具有相關權責權限的管理高層擔任。

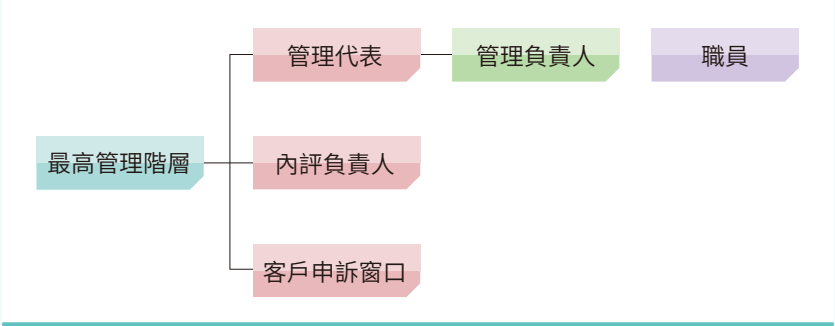


圖1｜管理小組例示圖

資料來源：本研究自製

▶實務案例◀

A為有線電視經營業者，擁有用戶資料高達上萬筆，因意識到近年來個資外洩事件頻繁與消費者意識抬頭，為了使公司用戶個資有完善之保障，避免產生個資外洩事故，破壞公司聲譽，決定導入個人資料保護與管理制度來改善公司現況，同時又能符合主管機關之要求，正所謂一兼二顧。於是次日即叫來公司唯一之法務人員B，請B於一個月內建立個人資料安全維護事項，並要完成全公司之個資盤點與風險評估。B原本於公司就身兼數職，任何與法律相關之案件皆會落到他頭上，現在又多了個資管理制度導入，讓其困擾不已，找其他單位來開會，大家都用公務忙碌推拖。最後，B因為無法承受過多業務量而選擇離職。

▶個資法遵建議◀

個資保護 人人有責

- 個資管理制度之建置不能僅靠單一部門，實務上執行應該由各部門共同推動建置比較適合。組織應配置管理人員與相當資源，才有能力執行個資管理制度，並且辦理個資安全維護事項。細部分工與職責規劃可依據公司實際狀況組成，基本上建議各部門主管與業務人員，以具備管理代表、管理人員及內評人員三種功能成員為個資管理小組編制概念核心，進行任務編組。
- 前面的案例中，雖然公司經營者A有意識個資制度建立之重要性，但是除了指派專人負責個資保護相關事宜外，應該還要授命由各相關部門同仁組成之個資保護小組一同進行，才能使個資保護制度有效推動，否則僅靠法務單位一人建置不僅人力不足，往往無法有實質權力協調各單位配合推動，且法務單位通常專精於法律事務，對於各單位實際執行業務蒐

集處理及利用個資狀況並不一定明瞭，於相關業務個資盤點時易有疏漏之處，故應該由公司各部門推派代表進行較為適當。

二、個人資料安全維護系統建置第二步驟：界定個人資料檔案盤點的範圍

雖然大家都知道要保護個人資料，但組織內部有什麼資料是需要保護的呢？有哪些資料是不需要特別保護的呢？

如果不知道有什麼資料要保護，將會不知該從何做起。因此，必須先瞭解個人資料的定義，並且將屬於個資法所保護的資料，透過一定的盤點方法，確認組織內部目前掌握及保存個資的情況，以確保個資保護沒有疏漏。

(一)個資盤點範圍

個人資料的保護範圍，包含自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

值得注意的是，可以「直接識別」的個人資料，是指資料本身具有高度的識別性，可以直接透過資料指涉特定個人。而「間接識別」是指，沒有辦法藉由資料本身來辨別指涉對象，須與透過其他資料對照、組合、連結等方式，才能識別資料所指涉的對象。

個資法小法典 個人資料保護法第2條第1款、個人資料保護法第3條

▶實務操作提醒◀

個資排排坐 未盤容易錯

實務上組織所掌握的個人資料是非常多元的，除了基本的員工個人資料與消費者個人資料以外，時常被忽略的部分，包括訪客登記表、領據、臉書私訊小編報名活動及委外廠商滿意度調查表等，只要是個資法所保護的個人資料，都應該納入個人資料盤點清冊，以防疏漏。

▶實務案例◀

某C電視購物頻道，在消費者進線時沒有提供個資蒐集使用及處理的告知聲明，只有在消費者訂單成立之後才提供告知聲明給消費者，並表示訂單成立之前不會儲存任何消費者個資，所以不需要事先提供告知聲明。雖然電視購物頻道業者認為，單純的以錄音方式紀錄與消費者間的對話，應該不需要先行告知聲明，但在電話的對話內容中，往往已經包含了個資。

▶個資法遵建議◀

- 前面的案例中，首先應該確認電視購物消費者錄音是否為個人資料。而確認消費者錄音是否屬於個人資料，需要透過錄音內容是否能直接或間接識別當事人進行判斷。從案例中之情形來看，消費者於進線時的錄音內容包括：購物台客服人員與消費者確認姓氏與稱謂等基本資料。而電視購物電話進線時客服人員端也會顯示消費者的電話號碼。電視購物業者可以透過結合相關消費者的綜合資訊，以間接識別的方式識別當事人。
- 以個資管理法遵實務角度來看，針對案例的情況，會建議在電話進線開始錄音前先進行個資告知聲明。

(二)釐清蒐集、處理及利用個人資料之目的

蒐集個人資料必須基於特定目的，組織因業務需求而蒐集、處理或利

用消費者個人資料時，除了必須基於特定目的外，同時必須符合個資法的要求，在該特定目的必要範圍內，為相關個資蒐集、處理及利用行為。

「目的外利用」應符合法定情況，若組織將原特定目的蒐集、處理及利用之個人資料，作於目的外的使用時，就會落入個資法上所稱「目的外利用」的情況。

以一般網站會員申請個資聲明為例，如果取得會員之個人資料，原本的目的只是為了會員管理，而個資聲明中也聲明「個人資料僅用於會員管理」，但後續卻想將這些個人資料用來進行消費喜好研究分析或行銷，這種超出原本個資蒐集目的使用，即屬於「目的外利用」。

若要對個人資料進行目的外利用，必須至少符合下列任一種情況，方得使用：

1.法律明文規定。

2.為增進公共利益所必要。

3.為免除當事人之生命、身體、自由或財產上之危險。

4.為防止他人權益之重大危害。

5.公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

6.經當事人同意。

7.有利於當事人權益。

個資法小法典 個人資料保護法第19條、個人資料保護法第20條

▶實務操作提醒◀

組織在建立「個資盤點清冊」時應該呈現的內容包含：

・資料是在什麼作業過程中進行蒐集、處理、利用；

・這筆資料包含哪些資料種類；

・資料的蒐集來源為何，可用以判斷資料為直接或間接蒐集；

・蒐集之特定目的為何，機關內部目前保管的部門以及場所；

・資料的保存期限；

・該資料是否會委託他人進行蒐集、處理或利用。

實務上組織在執行個人資料檔案盤點時，常常無法輕易的區別蒐集個人資料的特定目的，若能在盤點清冊上標明其代號，常見特定目的例如：〇九〇為消費者、客戶管理與服務；一三六為資(通)訊與資料庫管理；類別C〇〇一為辨識個人等，將有助於確認個人資料蒐集種類、特定目的及程序的關聯性與合法性。

▶實務案例◀

D電信公司企業文化相當重視個人資料保護，法務人員為了避免掛一漏萬，便在撰寫公司隱私權政策說明特定目的的地方，直接將法務部公告的「個人資料保護法之特定目的及個人資料之類別」中與公司營運有關係的所有目的，最大限度的都先放入特定目的之內容，例如〇四〇行銷、〇六九契約、類似契約或其他法律關係事務、〇七二政令宣導、〇八一個人資料之合法交易業務、〇八五旅外國人急難救助、〇九〇消費者、客戶管理與服務等。

由於電信公司實際業務目的應該是契約、類似契約關係、行銷及一般

消費者客戶管理。因此，D公司可能不適合以外國人急難救助作為蒐集個人資料的特定目的。

▶個資法遵建議◀

- 特定目的應以實際業務目的盧列即可。若於法務部所公布的「個人資料保護法之特定目的及個人資料之類別」找不到適合之項目，建議應該要將蒐集、處理及利用個人資料的特定目的清楚地合理闡述。
- 實務上很常見的情形是許多組織將大部分可能用到之特定目的匡列進去，但過於寬鬆的特定目的，難以使當事人了解蒐集的真正目的，因此個資法遵上建議特定目的應該扣合業務執行範圍，也不要用「…」或「包含但不限於」等不明確之用語。總而言之，特定目的的匡列應該以當事人能夠清楚且明白瞭解蒐集個人資料之目的為準。

(三)個資盤點方法與範例

實務上個資盤點之作法很多，沒有保證完全無疏漏的方法，但組織進行個資盤點時，大多建議以分析個資蒐集使用流程著手，盤點出公司所蒐集、處理以及利用的個人資料。這種方式可以比較精準的掌握組織蒐集使用個資的狀態，比較不容易有疏漏，也可以降低漏盤風險。

盤點其內容包括下列項目：

1.整理組織各作業流程中所保有的各類文件、檔案、簿冊，清查確認其是否含有個人資料。

2.清查所有涉及個人資料的文件，歸納整理成個人資料檔案，並建立個資盤點清冊。

3.使用個資盤點清冊檢視組織保存的個人資料種類、確認個人資料檔案名稱、保存的特定目的及依據，以及保存現況。

4.使用個資盤點清冊檢視並確認，在平常業務的蒐集、處理及利用個人資料的過程當中，是否有違法的可能。

5.組織建立個資盤點清冊將個人資料檔案盤點檢視之成果。

6.製作個資盤點清冊並妥善保管且定期維護。

※個資盤點清冊範例參照附錄四

▶實務操作提醒◀

除了一開始建置個人資料管理制度時，需要進行個資盤點，更應該每年定期進行個人資料盤點。除此之外，若公司有新增業務或有業務變更終止時也應進行更新，並維護先前所建立的個資盤點清冊，藉以確實呈現組織當前個資管理現況。

▶實務案例◀

某 E 電信業者將客戶網路申裝與滿意度調查統一委外給 F 廠商進行一併作業， F 廠商針對客戶需求裝機完成後，將會請客戶簽名確認申裝服務已順利完成，並且同步給客戶填寫滿意度調查表。滿意度調查表上有該客戶申裝案號、姓名、年齡及產品訊息。惟 E 電信業者於年度個資盤點時卻忽略委外申裝與滿意度調查作業，未於個資盤點清冊中呈現，直至外部單位來查核時才發現缺失。

▶個資法遵建議◀

- 個資漏盤是實務上常見的缺失，尤其常發生於新拓展或委外處理的業務。
- 我國個資法規定，在個資法適用範圍內，受委託蒐集、處理或利用個人資料的單位，執行蒐集、處理或利用個人資料的行為，視同委託機關的行為。

- 一般公司常認為委外處理就不用將該業務納入個資盤點是錯誤的觀念。委外的個資相關業務仍要納入盤點範圍，尤其近年來常見發生委外廠商個人資料外洩事故，應更加注意。
- 個人資料管理制度上，建議於各部門個資盤點後，應該再由主要推動個資管理制度之單位或公司內部的稽核單位進行複查，避免有漏盤之狀況發生。

個資法小法典 個人資料保護法第4條

三、個人資料安全維護系統建置第三步驟：建立個人資料風險評估及管理機制

組織完成個資盤點後，可以比較清楚的掌握企業內部所擁有的個人資料範圍。為了正確評估並有效管理個人資料檔案可能面臨的風險，應建立個人資料的風險評估與管理機制，並執行個人資料風險評估與管理作業。

個人資料之風險評估與管理機制，可以分為風險評估與風險管理兩部分。

(一)風險評估

「風險評估」的目的在於識別可能導致風險發生的原因(包含本身的弱點與可能的威脅來源)。風險的發生可能來自四面八方，無論來自內部或外部、天然的或人為，惡意或非惡意，都可能形成風險。風險通常會利用組織或資產的弱點，對組織造成潛在損害或實質上的損失。

目前實務上最常發生的情形，像是來自組織外部、人為的且惡意的駭客入侵。另外，還包含利用組織或資產本身所存在的弱點，間接導致損害的產生，例如紙本文件具有易燃、方便攜帶的特性，而毀損、滅失或竊取含有個人資料的紙本文件。

關於風險評估之具體標準及實務作法，可參考經濟部標準檢驗局公布的CNS 27005「資訊技術－安全技術－資訊安全風險管理」與CNS 31000「風險管理－原則與指導綱要」等國家標準。

(二)風險管理

「風險管理」是針對個人資料所面臨的可能風險，提出相對應的管理策略。組織針對其保有之個人資料風險評估出來後，即可找到自身弱點所在，進而研擬風險對策進行管控。

參照經濟部標準檢驗局所公布的國家標準，內容包含下列4項處理原則：

1.風險修改

在符合風險評鑑及風險處理要求下，選擇適切及經過衡量的控制措施，以管理風險。控制措施內容可以是矯正、消弭、預防、偵測及監視等方式。藉由施行、移除或改變控制措施可管理風險等級，進而使殘餘風險被控制在可接受範圍。

2.風險保留

風險經評估過後，若特定的風險明顯符合組織內部個人資料管理政策的風險接受準則，則該風險可以保留，但建議組織可以預先提撥風險準備金，用以確保風險結果實現時，能支應相關費用與損害賠償。

3.風險避免

當特定風險持續增加或持續發生，而且接受或保留風險可能會為組織帶來損失或不利影響時，應該規劃避免風險的措施(包括避免產生風險的情形繼續發生，或變更目前產生風險的運作情形)。例如將實體檔案或

儲存媒體存放於上鎖空間中；設置防火牆等機制；加強員工個資保護相關教育訓練等。

4.風險分擔

經過風險評估後，可以將特定風險結果請求第三方進行有效管理。例如透過分包方式將監視資料系統的風險，轉交由資訊安全機構協助相關業務。值得注意的是，組織所管理風險的賠償責任，無法透過分包方式轉由第三方承擔。

個資法小法典 CNS 27005「資訊技術—安全技術—資訊安全風險管理」
CNS 31000「風險管理—原則與指導綱要」

四、個人資料安全維護系統建置第四步驟：訂定個人資料安全維護規定

(一)個人資料侵害事故預防、通報及應變作業程序

依照個資法施行細則與安全維護辦法，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(下稱事故)，應訂定下列應變、通報及改善機制：

- 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。
- 事故發生後應受通報之對象及其通報方式。
- 事故發生後，其改善措施之研議機制。

另外應注意的是，當非公務機關遇到「重大個人資料事故」時，應即通報國家通訊傳播委員會。所謂「重大個人資料事故」是指個人資料遭竊取、

竄改、毀損、滅失或洩漏，將危及非公務機關正常營運或大量當事人權益的情形。

縱然有再周延的個資保護措施，個資事故發生的風險始終存在，因此依照上述規定制定並落實事故發生後的應變與通報等措施，才能夠在事故發生時，讓組織內部人員迅速應對，確保讓損害降到最小。

個資法小法典 個人資料保護法施行細則第12條第2項第4款
安全維護辦法第4條

▶實務操作提醒◀

個資事故通知

當組織發生個資事故時，組織應查明後以適當方式通知個資當事人，通知的內容至少應包含個人資料被侵害的事實及組織已採取的因應措施。

通知個資當事人的方式可以透過言詞、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。當前述通知方式需要的花費過鉅的時候，組織在斟酌技術的可行性與當事人隱私的保護情況下，可以透過網際網路、新聞媒體或其他適當公開方式為之。

※個資事故通知範本參照附錄五

有備無患 迅速防堵

除了避免個資事故發生之相關安全措施，組織應於事前訂定個資事故緊急應變措施，以防個資事故發生時可緊急應變處理，於短時間將損害降至最低。實務上常見組織訂有個資事故緊急應變之程序，但實際內容卻

無明確通報窗口與運作機制，這樣會導致事故發生時組織內部無法有效應變。

個資事故緊急應變措施應該有明確的流程，如此一來才能於事故發生的第一時間緊急處理。另外，組織所訂定之個資事故緊急應變措施，關於通報部分，往往僅有規定內部通報，而疏忽個資法通知當事人部分。

其實多數企業組織原本就有相關緊急應變程序，例如工安通報機制或資安通報事故，個資事故通報亦可直接適用類似之架構與方法為之，不用再建立新的通報制度。

▶實務案例◀

G為H電信業者的個資管理人員，負責公司個資管理制度程序書之撰寫與維護更新。鑑於近來同業發生重大個資外洩，造成當事人損害，造成該公司商譽嚴重受影響。所以G打算針對個資事故緊急應變程序再多加著重，特別是個資事故發生當事人通知之部分。但卻發現公司相關程序規範為「對於個人資料遭竊取之當事人，以書面通知……」，將通知當事人之事故限縮於「個人資料遭竊取」，涵蓋範圍與個資法規定之事故類型不符合。

▶個資法遵建議◀

- 我國個資法規範個資事故之態樣，並非侷限於竊取而已，其明定公務機關或非公務機關違反個資法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。
- 針對個資事故當事人通知部分不能僅規範竊取而已，應該要符合個資法規範，包含竊取、洩漏、竄改等其他侵害才是。況且近年來亦常發生竄改當事人資料使其受損害之案例，若組織對此未有事故緊急應變措施，可能使當事人損害加重。

- 通知個資事故當事人的方式並不只限於「書面」，組織於通知時，可以靈活運用言詞、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的方式。如果組織將相關程序規範限定為「以書面通知……」，則可能大幅提高組織通知個資事故當事人所需支出的費用。
- 對於事故通知當事人之內容應該要明確，並以書函、簡訊等方式通知當事人個人資料被侵害之事實、事故經過、個人資料處理情形及事後所採取之因應措施等。若遇有重大個人資料事故者，應即通報主管機關。相關人員事後需檢討事故發生之原因並研擬預防措施，對於因個資事故可能發生之訴訟或損害，也應該加以分析評估。

個資法小法典 個人資料保護法第12條

（二）符合個資法相關法令規定之內部管理程序

依照我國個資法與安全維護辦法，通傳產業者應就下列事項，訂定個人資料之管理程序：

- 蒐集、處理或利用之個人資料包含個資法第6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。
- 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。
- 檢視個人資料之蒐集、處理，是否符合個資法第19條規定，具有特定目的及法定情形；其經當事人同意者，並應確保符合個資法第7條第1項規定。

- 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，並應確保符合個資法第7條第2項規定。
- 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。
- 委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人依個資法施行細則第8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。
- 進行個人資料國際傳輸前，檢視是否受國家通訊傳播委員會相關法令限制並遵循之。
- 當事人行使個資法第3條所定權利之相關事項：
  - ◇ 當事人身分之確認。
  - ◇ 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。
  - ◇ 對當事人請求之審查方式，並遵守個資法有關處理期限之規定。
  - ◇ 有個資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。
  - ◇ 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，應依個資法第11條第1項、第2項及第5項規定辦理。
  - ◇ 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，應依個資法第11條第3項規定辦理。
  - ◇ 設置聯絡窗口供當事人申訴與諮詢。

▶實務操作提醒◀

- 組織除了訂定個資法相關法令規定之內部管理程序，最重要的是要遵守程序規範。個資管理制度上著重「說、寫、做」三者需一致，也就是程序書、人員認知與實際執行方式要同一。實務上常見空有內部管理程序，卻無落實、程序書規範和組織內部執行不一，或是程序書與內部業務根本無法扣合，這在個資管理制度上都不是有效管理，也容易造成管理上風險。
- 委外管理也是實務上常被忽略的部分，組織於程序書上往往制定相當嚴謹之管理規範，例如每半年對委外廠商進行查核、委外廠商合作終止後會進行個資刪除銷毀，但實際上卻無執行，造成個資管理上之漏洞，需加以注意。
- 實務運作上，組織之隱私權政策、隱私權聲明或是公告，都必須納入上述有關個資法之管理事項。並且建立文件化之程序。隱私權公告與個資告知聲明，應確保在蒐集個人資料之前，提供給當事人或讓其能顯而易見。例如業者為了受理民眾申辦電信相關業務，可於業者門市現場明顯處，以立牌方式公告說明其隱私權聲明，以達到告知隱私權政策的目的。
- 個資告知聲明要清楚說明，明確包含以下內容，如：機關名稱、蒐集目的、個資類別、個資使用方式及個資當事人權益等。須特別注意的是，對於蒐集目的的說明不應該模糊，或以概括方式表述。如果告知的內容並不符合實際個資蒐集使用情形，可能就不符合「明確告知」規定。因此，業者提供給個資當事人的個資聲明，必須因應不同業務內容，調整使用目的說明。

※告知函範本參照附錄六

個資法小法典 個人資料保護法第8條

▶實務案例◀

Ｉ電視購物業者為了增加公司營收，讓業績達新高峰，開發一款新APP讓消費者能快速於手機完成單手下單消費，不用再一直等待進線，增加多元消費管道。但同樣為加入會員之流程，公司官網與APP所蒐集之個人資料目的與種類並無不同，且最終皆匯入同一資料庫做會員管理，官網與APP隱私權聲明卻有出入不一致之情況。實際加入會員流程中有蒐集消費者生日，卻沒有在APP版隱私聲明中提及。個資蒐集目的的說明也有差異，明明有行銷事實，公司APP上也沒有告知消費者。

▶個資法遵建議◀

・如前述案例，實務上常見到明明是同一的公司的相同業務，網站入口的隱私權政策與APP入口的隱私權政策卻不同。這時候需進一步確認是因為具體蒐集、處理或利用個人資料之行為有所差異，還是僅為疏漏。通常同一業務的個資流程應為相同，隱私權政策應該要一致。

・為了避免網站入口的隱私權政策與APP入口的隱私權政策出入或版次不一之情形發生，建議組織於管理制度流程中增加隱私權政策與個資告知聲明定期檢視，以及相關的變更之機制。

(三)個人資料安全管理程序

個人資料安全管理的程序，包含資料安全管理、人員管理與設備安全管理。組織可從這三個面向著手個人資料安全的管理，確保個人資料檔案的安全，避免個人資料遭有心人士竊取、竄改、毀損、滅失或洩漏。

以下將就這三個面向說明組織應注意的事項：

1.資料安全管理

・訂定個人資料儲存媒體使用規範並確實執行。

- 個人資料儲存媒體於廢棄或轉作其他用途前，應以適當方式銷毀或確實刪除該媒體中所儲存之個人資料，確保個人資料完全移除，避免洩漏。委託他人執行上開行為時，也應依個資法施行細則第8條為適當監督。
- 蒐集、處理或利用個人資料時，如有加密或遮蔽之必要，應採取適當之加密或遮蔽機制。
- 傳輸個人資料時，針對不同的傳輸方式，組織應有相對應的適當安全防護機制。
- 依據所保有個人資料之重要性，採取適當之備份機制，同時對備份資料也必須予以適當保護。
- 採取適當之安全機制，避免用以蒐集、處理或利用個人資料之電腦、相關設備或系統遭無權限之存取或發生個資事故，例如：
  - ◇就個人資料之存取權限，設定必要之控管機制，並定期確認控管機制之有效性與適當性。
  - ◇安裝與建置防毒軟體、防火牆、入侵偵測系統（Intrusion Detection System, IDS）與入侵預防系統（Intrusion Prevention System, IPS）。
  - ◇使用多因素認證機制（Multi-Factor authentication, MFA），同時帳號密碼應符合一定複雜度並定期更換。
  - ◇涉及個人資料的系統變更時，應確保其系統的安全性並未降低。
- 定期確認蒐集、處理或利用個人資料之電腦、相關設備或系統具備必要之安全性，包括但不限採取適當之安全機制，因應惡意程式及系統漏洞所造成之威脅。例如：
  - ◇定期更新病毒碼與執行掃毒作業。
  - ◇定期針對系統與程式漏洞安裝修補程式，倘遇有重大更新時，應即時安裝修補程式。

・進行軟硬體測試時，應避免使用實際個人資料。如確有使用實際個人資料之必要時，應明確規定其使用之程序及安全管理方式。

・定期檢查使用於蒐集、處理或利用個人資料之電腦、相關設備或系統之使用狀況及個人資料存取之情形。同時也必須設定異常存取個人資料行為的監控機制。

2.人員安全管理

・確認蒐集、處理及利用個人資料的相關業務流程的負責人員。

・依據執行業務的必要，建立管理機制，設定組織所屬人員關於個人資料蒐集、處理或利用，及接觸個人資料儲存媒體之相關權限，定期檢視權限設定內容之必要性與適當性，並控管接觸個人資料之情形。

・要求所屬人員妥善保管個人資料的儲存媒介物，並與所屬人員約定保密義務（包含在職時與離職後的保密義務）。

・當所屬人員離職時應確保取消其存取權限，並要求將執行業務所持有保管的文件與資料辦理交接，不得攜離使用。

3.設備安全管理

・依據作業內容及環境之不同，實施必要之安全環境管制。

・妥善維護並控管個人資料蒐集、處理或利用過程中所使用之實體設備。

・針對不同作業環境，建置必要之保護設備或技術（例如設置監視器與門禁）。

個資法小法典 個人資料保護法施行細則第12條第1項
個人資料保護法施行細則第12條第2項第6款、第8款

▶實務操作提醒◀

- 個資法中所謂的適當安全措施，並非要求組織應一律以最高保護規格保護組織所保有的個人資料，而是組織應判斷其內部所保有的個人資料風險，依據風險評鑑的結果，同時考量組織內部運作的效率，選擇相對應的適當安全措施，並與所欲達成之個資保護目的間具有適當比例為原則。
- 實務上常見組織未經評估衡量，直接將個人資料安全管理程序程序用高規管理，但卻沒有資源或人力可以確實執行，如此僅為空泛程序無法有效管理，不是個資管理制度所要求的個人資料安全管理程序，有效的管理程序應要視組織風險評估採取適切管理模式。
- 法院實務上也會考量組織規模，判斷組織是否已採行適當安全措施，曾有組織於個資事故的民事損害賠償案件中主張其已採取防火牆、電子加密系統、封包加密處理與員工個人電腦防毒軟體等安全保護措施，也定有電腦使用管理辦法與舉辦資訊安全教育訓練，然而法院認為考量該組織規模與蒐集處理的個人資料數量，組織前述的安全防護措施只是基本配備（臺灣臺北地方法院107年度北小字第266號民事判決參照），因此組織仍應依循個資法及其施行細則與安全維護辦法規定，定期辦理個資盤點與風險評鑑，如此才能識別風險，並進而對症下藥。

個資法小法典 個人資料保護法施行細則第12條第2項

▶實務案例◀

J電信公司為了方便用戶續約，直接將特惠續約方案以簡訊方式發送給用戶，簡訊內容含有網頁連結，網址為該公司網頁與消費者手機號碼組

成，點進連結則可直接看到該用戶之會員資料並可選擇直接續約，但由於該公司發送之簡訊網址連結為公司網頁與用戶手機號碼明碼組成，網址末端即為用戶之手機號碼，點進去即可看到其個人資料，造成有心人士只要變更網址手機號碼連結，即可清楚獲得他人個資，造成重大資安漏洞，該公司用戶個資亦因此被他人不當存取。

▶個資法遵建議◀

- 組織除了訂定個人資料安全管理程序，更應有相關管控與檢核程序，以避免前述案例發生。該案並不是遭受重大惡意攻擊，僅是廠商於相關業務服務功能設計時未將個資隱私考量進去，造成個資與資安上之問題。
- 近幾年隨著科技日益進步，大多商業模式往往為結合個人資料與新興科技運用而生，故相關業務服務功能設計是否有涵蓋個人資料之隱私保護亦格外重要，應該從業務服務功能設計時就將隱私報護納入考量。
- 組織於開發產品時，應一併考量隱私保護設計，如此一來則能避免個資隱私保護之疑慮。另外，新產品或新服務提供前，內部應要訂定檢核機制，避免有疏漏之處。如上述J公司之案例，只要於事前有設立相關檢核人員進行確認，即可避免問題發生。

（四）國際傳輸

我國個資法針對個人資料的國際傳輸，是採取「原則開放，例外禁止」的規定。原則上，非公務機關可以進行國際傳輸個人資料，但是涉及下列情形時，中央目的事業主管機關（例如國家通訊傳播委員會），可以限制非公務機關進行個人資料國際傳輸：

1.涉及國家重大利益。

2.國際條約或協定有特別規定。

3.接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。

4.以迂迴方法向第三國（地區）傳輸個人資料規避個資法。

國家通訊傳播委員會曾於101年9月25日發布通傳通訊字第10141050780號令，表示「衡酌大陸地區之個人資料保護法令尚未完備，因此限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區。」業者在進行個人資料國際傳輸應特別注意前述命令。此外，依照安全維護辦法，在進行個人資料國際傳輸前，也應該檢視該項傳輸是否受到國家通訊傳播委員會相關法令限制。

個資法小法典 安全維護辦法第5條第1項第7款

▶實務操作提醒◀

- 基於大陸地區個人資料保護法令尚未完備，國家通訊傳播委員會禁止通傳業者跨境傳輸至中國大陸，通傳業者在進行個人資料之國際傳輸時應該特別注意。
- 由於將個人資料進行國際傳輸，性質上依個案情節可能分別屬於個人資料的處理或利用，因此進行個人資料傳輸前，也必須依照個資法規定將相關事項告知個資當事人，例如個人資料所欲進行國際傳輸的區域、期間與對象。
- 若執行個人資料傳輸的是受委託的單位，委託機關也必須針對受委託單位執行個人資料國際傳輸情況進行適當監督。監督事項應該包含：

  ◇預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。

◇受託者就安全維護措施所採取之措施。

◇有複委託者，其約定之受託者。

◇受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。

◇委託機關如對受託者有保留指示者，其保留指示之事項。

◇委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。

個資法小法典 個人資料保護法施行細則第8條
個人資料法護法施行細則第12條第2項

(五)使用記錄、軌跡資料及證據保存

非公務機關對於個人資料的使用紀錄、軌跡資料及證據保存，應訂定相關機制並予以落實。這邊所指的機制應包含，為了執行個人資料檔案安全維護計畫及處理方法所定各種個人資料保護機制、程序及措施，所記錄的個人資料使用情況、軌跡資料及相關證據。

針對依個資法規定刪除、停止處理或利用所保有之個人資料後留存的紀錄，如刪除、停止處理或利用之方法、時間，或將刪除、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等資料，也必須訂定相關紀錄、證據保存機制，並加以落實。

個資法小法典 個人資料法護法第11條第3項
個人資料保護法施行細則第12條第2項第10款
安全維護辦法第6條

▶實務操作提醒◀

・個人資料保存應該有一定之期限，組織應依照該個人資料性質訂定。若有法定保存期間的規定，需依照法定保存期間保存以符合法規要求。

・國家通訊傳播委員會針對通傳產業資料保存有許多規定，例如：

◇有線廣播電視法第50條規定系統經營者對訂戶申訴案件應即妥適處理，並建檔保存六個月。

◇電信管理法第9條電信事業對於用戶或使用電信人使用電信服務所生通信紀錄及帳務紀錄，應確保紀錄正確，保存一定期間及應予保密；用戶查詢其通信紀錄及帳務紀錄時，應予提供。

◇行動寬頻業務管理規則第83條之2機房告警與錄影紀錄至少應保存六個月。

◇固定通訊業務管理規則第74條之6與行動寬頻業務管理規則第83條之5規定委外維運作業時應由電信設備機房員工全程監控，並將系統連線之操作指令完整記錄之，該紀錄檔應至少保存六個月。

這些國家通訊傳播委員會對資料保存期間之法定要求相關業者皆應遵守。

- 組織可依照個資保存之必要性，訂定相關保存期限，實務上許多業者會將會員資料定為永久保存，但基於個人資料保存必要性考量，不建議永久保存，應依法評估保存期限與後續利用行為是否妥當定之，否則在特定目的消逝後，皆應刪除銷毀。

4 Do—執行與落實

組織何時需要了解「個人資料安全維護事項」內容並予以實踐?

組織執行業務時蒐集、處理或利用個人資料需合法，在掌握個人資料期間，組織有義務避免其所蒐集、處理或利用之個人資料被竊取、竄改、毀損、滅失或洩漏。此時，組織需了解並執行「個人資料安全維護事項」。

「個人資料安全維護事項」

「個人資料安全維護事項」是為了防止個人資料被竊取、竄改、毀損、滅失或洩漏，所採取的技術上及組織上之措施。「技術上措施」的實踐，可包括針對組織內之設備採取安全管理措施，以於技術上避免個人資料受到侵害。「組織上措施」的實踐，可包括組織對其成員提供個人資料保護相關之認知宣導及教育訓練。實踐上，組織需要：

(一)依照內部成員對應的職務內容、執行計畫，成員於組織內之角色、職

務權限，分別辦理相對應之個人資料保護專業教育訓練，以確保組織內負責各項職務之成員，確切掌握職務內個人資料保護相關知識，以及避免個人資料侵害的應對措施。

（二）針對所有成員提供個人資料保護之教育訓練，訓練內容應要包括個人資料保護相關法令之規定，以及說明各成員對個人資料保護之責任範圍與各項個人資料保護之管理程序、機制及措施等要求。

個資法小法典 個人資料保護法施行細則第12條第1項
個人資料保護法施行細則第12條第2項第7、8款

▶實務操作提醒◀

- 組織應定期舉辦宣導個人資料法遵管理相關之教育訓練，以使成員均得瞭解個人資料管理制度之內容，以及個人資料保護之重要性，使個人資料管理制度得以有效執行。
- 亦有組織會採取定期寄發電子報給成員，在組織例行會議中宣布個人資料管理政策，或在組織資訊系統中之公共資料夾設置「個人資料保護專區」等方式，實踐個人資料保護認知宣導。
- 個人資料保護相關之教育訓練，組織除得自行培訓講師外，也可以委託外部專家講習，或者是指派組織內之相關成員參與外部訓練等方式進行。
- 辦理個人資料保護相關之教育訓練或講習時，組織應記得留存如課程簽到表或測驗成績等相關文件，以利後續之稽核時能順利提出有辦理教育訓練之佐證。

5 Check and Action—查核與改進

依照PDCA之精神，組織內規劃並逐步實踐個人資料保護相關安全維護事項的同時，亦應針對其規劃及實踐之個人資料保護相關措施進行**「查核」**（Check），並力求持續**「改進」**（Act）。

一、「查核」（Check）

組織因執行業務而合法蒐集、處理或利用個人資料時，應採取「個人資料安全稽核機制」，以確認及防止個人資料遭受被竊取、竄改、毀損、滅失或洩漏等侵害。實踐上，組織得定期或不定期確認個人資料安全維護事項的實施情形。如有發現不符合組織個人資料保護政策之事項時，應記錄違反組織內個人資料保護政策之情況，並分析該缺失發生之原因，進而評估採取何種矯正或預防措施，以改善個人資料安全維護計畫之有效性和效率，達採取資料安全稽核機制之目的。

二、「改進」(Act)

組織內個人資料安全維護事項之實施情形確認後，組織應採取措施整體持續改善個人資料之安全維護，以達個人資料保護之目的。實踐上，組織透過個人資料安全稽核機制所發現之缺失，並評估採取何種矯正或預防措施後，除應確實執行外，也應持續追蹤矯正或預防措施之實行狀況。同時，組織也得以實行狀況，針對組織內成員及其所負責業務範圍，進行滾動式調整，以求動態地實踐個人資料保護之相關政策、機制，達個人資料安全維護之整體持續改善之成果。

個資法小法典 個人資料保護法施行細則第12條第2項第9款
個人資料保護法施行細則第12條第2項第11款

▶實務操作提醒◀

- 組織在制定內部之個人資料安全稽核機制時，得考量「組織內部政策要求」，「組織將如何建立及維持稽核制度運行」，「組織如何進行監督和審查內部個人資料安全維護措施，以確保其有效性與效率」等層面，進行相關規劃。
- 個人資料安全稽核機制之內容，可包括稽核計畫之擬訂方式、稽核執行之內容、稽核員之資格與選任、受稽核單位應配合事項、稽核結果之審核及追蹤等事項，以確保個人資料安全稽核作業順利進行。

※個人資料保護與管理稽核檢查表參照附錄七

6 End—使用目的不存在之後該怎做

原則上，計畫中止後以下情形組織應主動或依個人資料當事人之請求，刪除、停止處理或利用該個人資料：

（一）組織如因業務規劃，導致先前合法蒐集、處理及利用個人資料之特定目的消失。

（二）組織個人資料保護政策規定的蒐集、處理及利用個人資料期限屆滿時。

但此原則例外情形如下：

（一）因組織執行職務或業務所必須。

（二）組織取得當事人書面同意得繼續處理或利用的狀況時。

實踐上，組織若因業務終止導致特定目的消失，進而著手刪除、停止處理或利用特定個人資料時，須記錄其刪除、停止處理或利用的方法、時間及地點。如果是因組織再造，而產生移轉特定個人資料的狀況時，除須

確認是否有移轉該個人資料之合法依據外，須確認接受該個人資料移轉之對象也具備相關合法依據。確認具備合法依據後，移轉個人資料時，應記錄移轉之原因，接受此個人資料移轉之對象、方法、時間、地點等資訊及接收者持有個資的合法依據。

個資法小法典 個人資料保護法第11條第3項

▶實務操作提醒◀

實務操作上最常發生的問題是，難以舉證資料是否已經確實刪除。為解決這個困境，建議組織得在刪除、銷毀個人資料與其相關載體（如公文夾、公用硬碟等）時，可採取全程錄影等有效紀錄銷毀軌跡的方式，保存完整刪除、銷毀的過程，以供未來查核時證明使用。

附錄一｜個人資料保護法

第一章　總則

第1條（立法目的）

為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。

第2條（用詞定義）

本法用詞，定義如下：

一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

二、個人資料檔案：指依系 統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

三、蒐集：指以任何方式取得個人資料。

四、處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

五、利用：指將蒐集之個人資料為處理以外之使用。

六、國際傳輸：指將個人資料作跨國（境）之處理或利用。

七、公務機關：指依法行使公權力之中央或地方機關或行政法人。

八、非公務機關：指前款以外之自然人、法人或其他團體。

九、當事人：指個人資料之本人。

第3條（不得預先拋棄或以特約限制）

當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：

一、查詢或請求閱覽。

二、請求製給複製本。

三、請求補充或更正。

四、請求停止蒐集、處理或利用。

五、請求刪除。

第4條（視同委託機關）

受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。

第5條（個人資料之處理行為）

個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

第6條（特種個人資料之保護）

有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

一、法律明文規定。

二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。

三、當事人自行公開或其他已合法公開之個人資料。

四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。

六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

依前項規定蒐集、處理或利用個人資料，準用第八條、第九條規定；其中前項第六款之書面同意，準用第七條第一項、第二項及第四項規定，並以書面為之。

第7條（書面同意之內涵）

第十五條第二款及第十九條第一項第五款所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。

第十六條第七款、第二十條第一項第六款所稱同意，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示。

公務機關或非公務機關明確告知當事人第八條第一項各款應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已依第十五條第二款、第十九條第一項第五款之規定表示同意。

蒐集者就本法所稱經當事人同意之事實，應負舉證責任。

第8條（直接蒐集個人資料應告知事項及免告知之情形）

公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：

一、公務機關或非公務機關名稱。

二、蒐集之目的。

三、個人資料之類別。

四、個人資料利用之期間、地區、對象及方式。

五、當事人依第三條規定得行使之權利及方式。

六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

有下列情形之一者，得免為前項之告知：

一、依法律規定得免告知。

二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。

三、告知將妨害公務機關執行法定職務。

四、告知將妨害公共利益。

五、當事人明知應告知之內容。

六、個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

第9條（間接蒐集個人資料之告知義務）

公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。

有下列情形之一者，得免為前項之告知：

一、有前條第二項所列各款情形之一。

二、當事人自行公開或其他已合法公開之個人資料。

三、不能向當事人或其法定代理人為告知。

四、基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。

五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。

第一項之告知，得於首次對當事人為利用時併同為之。

第10條（妨害重大利益要件之請求限制）

公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：

一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。

二、妨害公務機關執行法定職務。

三、妨害該蒐集機關或第三人之重大利益。

第11條（個人資料更正或補充及權責）

公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。

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。但因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議者，不在此限。

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、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。

違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。

因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。

第12條（個人資料遭違法侵害之通知）

公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

第13條（處理期限或延長）

公務機關或非公務機關受理當事人依第十條規定之請求，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。

公務機關或非公務機關受理當事人依第十一條規定之請求，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。

第14條（使用者付費）

查詢或請求閱覽個人資料或製給複製本者，公務機關或非公務機關得酌收必要成本費用。

第二章　公務機關對個人資料之蒐集、處理及利用

第15條（公務機關蒐集或處理個人資料之要件）

公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：

一、執行法定職務必要範圍內。

二、經當事人同意。

三、對當事人權益無侵害。

第16條（公務機關不得逾越執行法定職務之必要範圍）

公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：

一、法律明文規定。

二、為維護國家安全或增進公共利益所必要。

三、為免除當事人之生命、身體、自由或財產上之危險。

四、為防止他人權益之重大危害。

五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

六、有利於當事人權益。

七、經當事人同意。

第17條（提供民眾查閱之公開事項）

公務機關應將下列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：

一、個人資料檔案名稱。

二、保有機關名稱及聯絡方式。

三、個人資料檔案保有之依據及特定目的。

四、個人資料之類別。

第18條（個人資料檔案之安全維護）

公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

第三章　非公務機關對個人資料之蒐集、處理及利用

第19條（非公務機關蒐集或處理個人資料之要件）

非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：

一、法律明文規定。

二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。

三、當事人自行公開或其他已合法公開之個人資料。

四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

五、經當事人同意。

六、為增進公共利益所必要。

七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。

八、對當事人權益無侵害。

蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

第20條（非公務機關利用個人資料之除外情形）

非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：

一、法律明文規定。

二、為增進公共利益所必要。

三、為免除當事人之生命、身體、自由或財產上之危險。

四、為防止他人權益之重大危害。

五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

六、經當事人同意。

七、有利於當事人權益。

非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。

非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。

第21條（非公務機關為國際傳輸個人資料之限制）

非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：

一、涉及國家重大利益。

二、國際條約或協定有特別規定。

三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。

四、以迂迴方法向第三國（地區）傳輸個人資料規避本法。

第22條（行政監督之權責及保密義務）

中央目的事業主管機關或直轄市、縣（市）政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。

中央目的事業主管機關或直轄市、縣（市）政府為前項檢查時，對於得沒入或可為證據之個人資料或其檔案，得扣留或複製之。對於應扣留或複製之物，得要求其所有人、持有人或保管人提出或交付；無正當理由拒絕提出、交付或抗拒扣留或複製者，得採取對該非公務機關權益損害最少之方法強制為之。

中央目的事業主管機關或直轄市、縣（市）政府為第一項檢查時，得率同資訊、電信或法律等專業人員共同為之。

對於第一項及第二項之進入、檢查或處分，非公務機關及其相關人員不得規避、妨礙或拒絕。

參與檢查之人員，因檢查而知悉他人資料者，負保密義務。

第23條（扣留物或複製物之標示、保管及發還）

對於前條第二項扣留物或複製物，應加封緘或其他標識，並為適當之處置；其不便搬運或保管者，得命人看守或交由所有人或其他適當之人保管。

扣留物或複製物已無留存之必要，或決定不予處罰或未為沒入之裁處者，應發還之。但應沒入或為調查他案應留存者，不在此限。

第24條（不服聲明異議之權利及救濟）

非公務機關、物之所有人、持有人、保管人或利害關係人對前二條之要求、強制、扣留或複製行為不服者，得向中央目的事業主管機關或直轄市、縣（市）政府聲明異議。

前項聲明異議，中央目的事業主管機關或直轄市、縣（市）政府認為有理由者，應立即停止或變更其行為；認為無理由者，得繼續執行。經該聲明異議之人請求時，應將聲明異議之理由製作紀錄交付之。

對於中央目的事業主管機關或直轄市、縣（市）政府前項決定不服者，僅得於對該案件之實體決定聲明不服時一併聲明之。但第一項之人依法不得對該案件之實體決定聲明不服時，得單獨對第一項之行為逕行提起行政訴訟。

第25條（違反規定之裁處）

非公務機關有違反本法規定之情事者，中央目的事業主管機關或直轄市、縣（市）政府除依本法規定裁處罰鍰外，並得為下列處分：

一、禁止蒐集、處理或利用個人資料。

二、命令刪除經處理之個人資料檔案。

三、沒入或命銷燬違法蒐集之個人資料。

四、公布非公務機關之違法情形，及其姓名或名稱與負責人。

中央目的事業主管機關或直轄市、縣（市）政府為前項處分時，應於防制違反本法規定情事之必要範圍內，採取對該非公務機關權益損害最少之方法為之。

第26條（公布檢查結果）

中央目的事業主管機關或直轄市、縣（市）政府依第二十二條規定檢查後，未發現有違反本法規定之情事者，經該非公務機關同意後，得公布檢查結果。

第27條（個人資料檔案安全維護計畫及業務終止處理方法）

非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

中央目的事業主管機關得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。

前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。

第四章　損害賠償及團體訴訟

第28條（公務機關違法之損害賠償）

公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。

被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。

依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一事件新臺幣五百元以上二萬元以下計算。

對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。

同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受第三項所定每人每一事件最低賠償金額新臺幣五百元之限制。

第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。

第29條（非公務機關違法之損害賠償）

非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。

依前項規定請求賠償者，適用前條第二項至第六項規定。

第30條（請求損害賠償之時效）

損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同。

第31條（公務、非公務機關損害賠償之適用法）

損害賠償，除依本法規定外，公務機關適用國家賠償法之規定，非公務機關適用民法之規定。

第32條（團體訴訟之符合要件）

依本章規定提起訴訟之財團法人或公益社團法人，應符合下列要件：

一、財團法人之登記財產總額達新臺幣一千萬元或社團法人之社員人數達一百人。

二、保護個人資料事項於其章程所定目的範圍內。

三、許可設立三年以上。

第33條（損害賠償訴訟之管轄權）

依本法規定對於公務機關提起損害賠償訴訟者，專屬該機關所在地之地方法院管轄。對於非公務機關提起者，專屬其主事務所、主營業所或住所地之地方法院管轄。

前項非公務機關為自然人，而其在中華民國現無住所或住所不明者，以其在中華民國之居所，視為其住所；無居所或居所不明者，以其在中華民國最後之住所，視為其住所；無最後住所者，專屬中央政府所在地之地方法院管轄。

第一項非公務機關為自然人以外之法人或其他團體，而其在中華民國現無主事務所、主營業所或主事務所、主營業所不明者，專屬中央政府所在地之地方法院管轄。

第34條（損害賠償團體訴訟裁判費減免）

對於同一原因事實造成多數當事人權利受侵害之事件，財團法人或公益社團法人經受有損害之當事人二十人以上以書面授與訴訟實施權者，得以自己之名義，提起損害賠償訴訟。當事人得於言詞辯論終結前以書面撤回訴訟實施權之授與，並通知法院。

前項訴訟，法院得依聲請或依職權公告曉示其他因同一原因事實受有損害之當事人，得於一定期間內向前項起訴之財團法人或公益社團法人授與訴訟實施權，由該財團法人或公益社團法人於第一審言詞辯論終結前，擴張應受判決事項之聲明。

其他因同一原因事實受有損害之當事人未依前項規定授與訴訟實施權者，亦得於法院公告曉示之一定期間內起訴，由法院併案審理。

其他因同一原因事實受有損害之當事人，亦得聲請法院為前項之公告。

前二項公告，應揭示於法院公告處、資訊網路及其他適當處所；法院認為必要時，並得命登載於公報或新聞紙，或用其他方法公告之，其費用由國庫墊付。

依第一項規定提起訴訟之財團法人或公益社團法人，其標的價額超過新臺幣六十萬元者，超過部分暫免徵裁判費。

第35條（撤回訴訟之當然停止）

當事人依前條第一項規定撤回訴訟實施權之授與者，該部分訴訟程序當然停止，該當事人應即聲明承受訴訟，法院亦得依職權命該當事人承受訴訟。

財團法人或公益社團法人依前條規定起訴後，因部分當事人撤回訴訟實施權之授與，致其餘部分不足二十人者，仍得就其餘部分繼續進行訴訟。

第36條（損害賠償請求權）

各當事人於第三十四條第一項及第二項之損害賠償請求權，其時效應分別計算。

第37條（訴訟行為之限制）

財團法人或公益社團法人就當事人授與訴訟實施權之事件，有為一切訴訟行為之權。但當事人得限制其為捨棄、撤回或和解。

前項當事人中一人所為之限制，其效力不及於其他當事人。

第一項之限制，應於第三十四條第一項之文書內表明，或以書狀提出於法院。

第38條（自行提起上訴之要件及時期）

當事人對於第三十四條訴訟之判決不服者，得於財團法人或公益社團法人上訴期間屆滿前，撤回訴訟實施權之授與，依法提起上訴。

財團法人或公益社團法人於收受判決書正本後，應即將其結果通知當事人，並應於七日內將是否提起上訴之意旨以書面通知當事人。

第39條（不得請求訴訟所得之報酬）

財團法人或公益社團法人應將第三十四條訴訟結果所得之賠償，扣除訴訟必要費用後，分別交付授與訴訟實施權之當事人。

提起第三十四條第一項訴訟之財團法人或公益社團法人，均不得請求報酬。

第40條（訴訟代理人）

依本章規定提起訴訟之財團法人或公益社團法人，應委任律師代理訴訟。

第五章　罰則

第41條（罰則）

意圖為自己或第三人不法之利益或損害他人之利益，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。

第42條（罰則）

意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金。

第43條（罰則）

中華民國人民在中華民國領域外對中華民國人民犯前二條之罪者，亦適用之。

第44條（罰則）

公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。

第45條（告訴乃論）

本章之罪，須告訴乃論。但犯第四十一條之罪者，或對公務機關犯第四十二條之罪者，不在此限。

第46條（從重處罰）

犯本章之罪，其他法律有較重處罰規定者，從其規定。

第47條（罰則）

非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之：

一、違反第六條第一項規定。

二、違反第十九條規定。

三、違反第二十條第一項規定。

四、違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或處分。

第48條（罰則）

非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰：

一、違反第八條或第九條規定。

二、違反第十條、第十一條、第十二條或第十三條規定。

三、違反第二十條第二項或第三項規定。

四、違反第二十七條第一項或未依第二項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。

第49條（罰則）

非公務機關無正當理由違反第二十二條第四項規定者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣二萬元以上二十萬元以下罰鍰。

第50條（罰則）

非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。

第六章　附則

第51條（除外規定）

有下列情形之一者，不適用本法規定：

一、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。

二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。

公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。

第52條（委託及保密義務）

第二十二條至第二十六條規定由中央目的事業主管機關或直轄市、縣（市）政府執行之權限，得委任所屬機關、委託其他機關或公益團體辦理；其成員因執行委任或委託事務所知悉之資訊，負保密義務。

前項之公益團體，不得依第三十四條第一項規定接受當事人授與訴訟實施權，以自己之名義提起損害賠償訴訟。

第53條（特定目的及個人資料類別之訂定）

法務部應會同中央目的事業主管機關訂定特定目的及個人資料類別，提供公務機關及非公務機關參考使用。

第54條（告知義務及處罰）

本法中華民國九十九年五月二十六日修正公布之條文施行前，非由當事人提供之個人資料，於本法一百零四年十二月十五日修正之條文施行後為處理或利用者，應於處理或利用前，依第九條規定向當事人告知。

前項之告知，得於本法中華民國一百零四年十二月十五日修正之條文施行後首次利用時併同為之。

未依前二項規定告知而利用者，以違反第九條規定論處。

第55條（施行細則）

本法施行細則，由法務部定之。

第56條（施行日）

本法施行日期，由行政院定之。

現行條文第十九條至第二十二條及第四十三條之刪除，自公布日施行。

前項公布日於現行條文第四十三條第二項指定之事業、團體或個人應於指定之日起六個月內辦理登記或許可之期間內者，該指定之事業、團體或個人得申請終止辦理，目的事業主管機關於終止辦理時，應退還已繳規費。已辦理完成者，亦得申請退費。

前項退費，應自繳費義務人繳納之日起，至目的事業主管機關終止辦理之日止，按退費額，依繳費之日郵政儲金之一年期定期存款利率，按日加計利息，一併退還。已辦理完成者，其退費，應自繳費義務人繳納之日起，至目的事業主管機關核准申請之日止，亦同。

附錄二｜個人資料保護法施行細則

第1條

本細則依個人資料保護法（以下簡稱本法）第五十五條規定訂定之。

第2條

本法所稱個人，指現生存之自然人。

第3條

本法第二條第一款所稱得以間接方式識別，指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。

第4條

本法第二條第一款所稱病歷之個人資料，指醫療法第六十七條第二項所列之各款資料。

本法第二條第一款所稱醫療之個人資料，指病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方、用藥、施術或處置所產生之個人資料。

本法第二條第一款所稱基因之個人資料，指由人體一段去氧核醣核酸構成，為人體控制特定功能之遺傳單位訊息。

本法第二條第一款所稱性生活之個人資料，指性取向或性慣行之個人資料。

本法第二條第一款所稱健康檢查之個人資料，指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料。

本法第二條第一款所稱犯罪前科之個人資料，指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄。

第5條

本法第二條第二款所定個人資料檔案，包括備份檔案。

第6條

本法第二條第四款所稱刪除，指使已儲存之個人資料自個人資料檔案中消失。

本法第二條第四款所稱內部傳送，指公務機關或非公務機關本身內部之資料傳送。

第7條

受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之。

第8條

委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。

前項監督至少應包含下列事項：

一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。

二、受託者就第十二條第二項採取之措施。

三、有複委託者，其約定之受託者。

四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。

五、委託機關如對受託者有保留指示者，其保留指示之事項。

六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。

第一項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。

受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。

第9條

本法第六條第一項但書第一款、第八條第二項第一款、第十六條但書第一款、第十九條第一項第一款、第二十條第一項但書第一款所稱法律，指法律或法律具體明確授權之法規命令。

第10條

本法第六條第一項但書第二款及第五款、第八條第二項第二款及第三款、第十條但書第二款、第十五條第一款、第十六條所稱法定職務，指於下列法規中所定公務機關之職務：

一、法律、法律授權之命令。

二、自治條例。

三、法律或自治條例授權之自治規則。

四、法律或中央法規授權之委辦規則。

第11條

本法第六條第一項但書第二款及第五款、第八條第二項第二款所稱法定義務，指非公務機關依法律或法律具體明確授權之法規命令所定之義務。

第12條

本法第六條第一項但書第二款及第五款所稱適當安全維護措施、第十八條所稱安全維護事項、第十九條第一項第二款及第二十七條第一項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。

前項措施，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：

一、配置管理之人員及相當資源。

二、界定個人資料之範圍。

三、個人資料之風險評估及管理機制。

四、事故之預防、通報及應變機制。

五、個人資料蒐集、處理及利用之內部管理程序。

六、資料安全管理及人員管理。

七、認知宣導及教育訓練。

八、設備安全管理。

九、資料安全稽核機制。

十、使用紀錄、軌跡資料及證據保存。

十一、個人資料安全維護之整體持續改善。

第13條

本法第六條第一項但書第三款、第九條第二項第二款、第十九條第一項第三款所稱當事人自行公開之個人資料，指當事人自行對不特定人或特定多數人揭露其個人資料。

本法第六條第一項但書第三款、第九條第二項第二款、第十九條第一項第三款所稱已合法公開之個人資料，指依法律或法律具體明確授權之法規命令所公示、公告或以其他合法方式公開之個人資料。

第14條

本法第六條第一項但書第六款、第十一條第二項及第三項但書所定當事人書面同意之方式，依電子簽章法之規定，得以電子文件為之。

第15條

本法第七條第二項所定單獨所為之意思表示，如係與其他意思表示於同一書面為之者，蒐集者應於適當位置使當事人得以知悉其內容並確認同意。

第16條

依本法第八條、第九條及第五十四條所定告知之方式，得以言詞、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。

第17條

本法第六條第一項但書第四款、第九條第二項第四款、第十六條但書第五款、第十九條第一項第四款及第二十條第一項但書第五款所稱無從識別特定當事人，指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者。

第18條

本法第十條但書第三款所稱妨害第三人之重大利益，指有害於第三人個人之生命、身體、自由、財產或其他重大利益。

第19條

當事人依本法第十一條第一項規定向公務機關或非公務機關請求更正或補充其個人資料時，應為適當之釋明。

第20條

本法第十一條第三項所稱特定目的消失，指下列各款情形之一：

一、公務機關經裁撤或改組而無承受業務機關。

二、非公務機關歇業、解散而無承受機關，或所營事業營業項目變更而與

三、原蒐集目的不符。

四、特定目的已達成而無繼續處理或利用之必要。

五、其他事由足認該特定目的已無法達成或不存在。

第21條

有下列各款情形之一者，屬於本法第十一條第三項但書所定因執行職務或業務所必須：

一、有法令規定或契約約定之保存期限。

二、有理由足認刪除將侵害當事人值得保護之利益。

三、其他不能刪除之正當事由。

第22條

本法第十二條所稱適當方式通知，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。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。

依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。

第23條

公務機關依本法第十七條規定為公開，應於建立個人資料檔案後一個月內為之；變更時，亦同。公開方式應予以特定，並避免任意變更。

本法第十七條所稱其他適當方式，指利用政府公報、新聞紙、雜誌、電子報或其他可供公眾查閱之方式為公開。

第24條

公務機關保有個人資料檔案者，應訂定個人資料安全維護規定。

第25條

本法第十八條所稱專人，指具有管理及維護個人資料檔案之能力，且足以擔任機關之個人資料檔案安全維護經常性工作之人員。

公務機關為使專人具有辦理安全維護事項之能力，應辦理或使專人接受相關專業之教育訓練。

第26條

本法第十九條第一項第二款所定契約或類似契約之關係，不以本法修正施行後成立者為限。

第27條

本法第十九條第一項第二款所定契約關係，包括本約，及非公務機關與當事人間為履行該契約，所涉及必要第三人之接觸、磋商或聯繫行為及給付或向其為給付之行為。

本法第十九條第一項第二款所稱類似契約之關係，指下列情形之一者：

一、非公務機關與當事人間於契約成立前，為準備或商議訂立契約或為交易之目的，所進行之接觸或磋商行為。

二、契約因無效、撤銷、解除、終止而消滅或履行完成時，非公務機關與當事人為行使權利、履行義務，或確保個人資料完整性之目的所為之連繫行為。

第28條

本法第十九條第一項第七款所稱一般可得之來源，指透過大眾傳播、網際網路、新聞、雜誌、政府公報及其他一般人可得知悉或接觸而取得個人資料之管道。

第29條

依本法第二十二條規定實施檢查時，應注意保守秘密及被檢查者之名譽。

第30條

依本法第二十二條第二項規定，扣留或複製得沒入或可為證據之個人資料或其檔案時，應掣給收據，載明其名稱、數量、所有人、地點及時間。

依本法第二十二條第一項及第二項規定實施檢查後，應作成紀錄。

前項紀錄當場作成者，應使被檢查者閱覽及簽名，並即將副本交付被檢查

者；其拒絕簽名者，應記明其事由。

紀錄於事後作成者，應送達被檢查者，並告知得於一定期限內陳述意見。

第31條

本法第五十二條第一項所稱之公益團體，指依民法或其他法律設立並具備個人資料保護專業能力之公益社團法人、財團法人及行政法人。

第32條

本法修正施行前已蒐集或處理由當事人提供之個人資料，於修正施行後，得繼續為處理及特定目的內之利用；其為特定目的外之利用者，應依本法修正施行後之規定為之。

第33條

本細則施行日期，由法務部定之。

附錄三｜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

第1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。

第2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。

第3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。

第4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量當事人權益之情形。

第5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。

（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6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。

第7條

本辦法自發布日施行。

附錄四｜個資盤點清冊

盤點部門：　　盤點者：　　盤點負責人：

檔案編號	作業流程名稱	個資行為態樣(可複選) 1.蒐集 2.處理 3.利用 4.國際傳輸	個人資料			直接蒐集			間接蒐集			告知義務		委託或受託		保管儲存或刪除銷毀				數量(概數)
			檔案名稱	種類及類別	類型 1.紙本 2.電子檔 3.資料庫 4.其他	方式	特定目的	法定情形	來源	特定目的	法定情形	告知與否	免告知之法定事由	有無	委託書或受託者	資料載體	儲放場所	保存期限 1.法定 2.自訂 3.其他	刪除銷毀	

資料來源：本手冊自行繪製

附錄五｜個資事故通知範本

*以下僅供參考，實際內容應依安全維護辦法第3條規定，視實際事故情況及公司因應政策調整

個資事故通知範本（一）

親愛的使用者您好：

本公司近日接獲消費者告知有關詐騙集團以本公司網站名義及消費者相關個資進行詐騙。經本公司調查，該等疑似個資外洩事故可能來自於本公司系統的瑕疵，本公司在疑似個資外洩事故發生後，已先行修補，並確保系統已無相關瑕疵。此外，本公司也委託專業資訊廠商進行新版系統開發，確保個資保護機制能有效落實。

本公司致力於確保各位消費者使用本公司服務之良好體驗。若您有相關的建議與疑問，歡迎採以下聯絡管道與我們聯繫。

客服聯絡：0800-000-000

資料來源：本手冊自行繪製

個資事故通知範本（二）

親愛的會員您好

非常抱歉，由於您在今年的03月在本公司B網站購物消費，B網站近日因遭駭客入侵發生個人資料外洩事故，且已有消費者接獲詐騙集團電話。提醒您，如有接獲疑似詐騙電話，請不要聽從指示操作ATM或提供任何個人資料，請立即通報165警政署反詐騙專線，本公司已針對該個資事故進行系統升級與資訊安全加密保護，未來也會持續加強個人資料保護與資訊安全管理，以降低消費者個資被侵害的風險。如您有訂單問題或與本次事故之疑問，請於平日上班時間與本公司客服人員聯繫（02-0000-0000）。

資料來源：本手冊自行繪製

附錄六｜告知函範本

*以下僅供參考，實際內容應依安全維護辦法第3條規定，視實際業務及公司個資政策調整

個資蒐集告知聲明範本（一）

個人資料蒐集告知聲明

OO電信股份有限公司基於「契約履行」、「消費者／客戶／會員管理與服務」、「經營電信業務／電信加值網路業務」、「電子商務服務」、「行銷」、「調查、統計與研究分析」、「資通訊服務」等目的，須蒐集您的個人資料。您可依法向我們行使「查詢／閱覽／補充／更正個人資料」、「提供個人資料複本」、「要求停止蒐集／處理／利用個人資料」、「要求刪除個人資料」等權利。更多關於我們如何蒐集／處理／利用您的個人資料，以及您的權利行使等資訊，請見OO電信股份有限公司個人資料蒐集告知聲明（註：此處置入網頁連結或另放置QR code；或依該消費者之特性，也可寄送電子郵件或直接交付紙本）。

資料來源：108年通傳事業導入隱私保護管理機制與資料加值服務之研析委託研究_期末報告-上冊_附件2

個資蒐集告知聲明範本（二）

OO電信股份有限公司個人資料蒐集告知聲明

感謝您成為本公司的客戶，本公司重視您的隱私與個人資料保護，並尊重您的個人資料控制權。以下將說明本公司如何蒐集、處理、利用您的個人資料，以及您有哪些權利可以行使。請留意，如您不是申辦本服務之人（非契約當事人）但使用本服務時（由他人申辦但供您使用），以下內容也對您適用。申辦本服務之人有義務讓實際使用本服務之人詳閱以下內容。

1.誰在蒐集您的個人資料

OO電信股份有限公司（以下稱為「我們」）。

2.我們為什麼蒐集您的個人資料（蒐集目的）

（註：請再依實際情形補充或調整）

・履行契約義務及行使契約權利　　・履行法定義務

・消費者／客戶／會員管理與服務　・電子商務服務

・電信業務／電信加值網路業務　　・ 行銷

・調查、統計與研究分析　　・資（通）訊服務／資料庫管理／安全管理

3.我們蒐集您的哪些個人資料（註：請再依實際情形補充或調整下列內容）

・帳戶資訊

- 包含您的姓名、電話、地址、電子郵件信箱等在申請服務時提供的識別類及特徵類個人資料（須依法提供身分證明文件）。
- 其他與您申辦的服務有關，或您在使用過程產生的資訊，例如我們指配給您的號碼、通信紀錄、帳單紀錄、消費及繳費方式、服務歷程紀錄、服務或設備之識別代碼，以及其他與您的帳戶相關的個人資料。

・服務使用與效能資訊

包含可揭露您如何使用我們的服務，以及我們的服務效能之資訊。

・網路使用資訊

如果您使用我們的網路服務，我們將取得您的網路使用情形資訊，例如：

- 您的ip位址
- 您造訪的網頁之資訊（例如瀏覽網址、造訪及停留時間等）。
- 您的行動裝置應用程式使用資訊（例如應用程式名稱、使用情形等）。

・位置資訊

如您使用我們的電話或網路服務，我們將取得您的地理位置資訊。

・其他服務資料

如您已經或在將來成為我們其他服務的客戶／會員，我們可能會將您的個人資料與其他服務之資料串接整併。

4.我們如何利用您的個人資料（註：請再依實際情形補充或調整下列內容）

4.1 期間及地區

我們會在您使用本服務（保有帳戶）的期間與地區內利用您的個人資料。當本契約終止或解除（您不再使用本服務）後，我們會在法令要求或許可

的範圍與期限內保留及利用您的個人資料，並在該期限後，以無法識別您的身分之形式保存您使用本服務期間所提供或產生的資料。

4.2 利用個人資料之方式與對象

我們會以必要的方式利用您的個人資料以達成蒐集目的，例如：

- 為您建立客戶／會員檔案以便我們管理帳戶。
- 為提供客戶服務而以您的各項聯繫方式與您為業務聯繫（包含寄送商品）、向您通知與您申辦之服務有關的資訊，或回覆您的提問、申訴。
- 寄送帳單／催繳訊息至您的地址或電子郵件信箱；藉由電話聯繫或簡訊通知您有關繳費／催繳之資訊。
- 以您的各項聯繫方式向您提供行銷資訊，例如優惠方案、促銷活動、我們的其他服務，以及其他更適合您的服務方案等。
- 分析您的個人資料以維持、保護、開發及增進我們的服務。
- 分析您的個人資料以依分析結果向您推薦我們提供的其他您可能有興趣或適合您的商品／服務。
- 分析您的個人資料，並以統計數據、趨勢或其他無法識別您的身分之形式產出結果，對外提供給我們的企業客戶（例如讓企業客戶瞭解他們的門市熱點、消費者年齡／性別分布、消費者停駐時間等）。

  將您的個人資料提供給受我們委託的第三人（例如行銷／分析／調查／廣告／公關業者、物流業者、金流業者、資訊服務業者等），在受委託的範圍內協助我們達成蒐集目的。我們會對受委託的第三人執行必要的監督，以確保您的個人資料安全
- 違約行為的預防、調查與權利行使。

4.3 蒐集目的以外的利用（註：非我國個資法要求應告知之內容，但適當揭露有助於提升透明度）

我們只會在蒐集目的之必要範圍內，依前述說明利用您的個人資料，除非：

- 法律明文規定。例如受司法機關或主管機關依法要求提供個人資料。
- 為增進公共利益所必要或為防止他人權益之重大危害。例如為維護網路完整性、確保網路與裝置安全、偵測／預防詐欺或網路犯罪等違法行為。

- 為免除您的生命、身體、自由或財產上之危險。例如當您行蹤不明時，將您的位置資訊提供給有權得知之第三人。
- 受公務機關或學術研究機構請託，基於公共利益為統計或學術研究而有必要，以無法識別您的身分之形式，提供資料給該公務機關或學術研究機構；或以可識別您的身分之形式提供資料，但該公務機關或學術研究機構保證所產出並對外揭露之結果無法識別您的身分。
- 依法得到您的同意。
- 有利於您的權益。

5.您有哪些權利可以行使

- 您有權請求查詢、閱覽我們保有您的個人資料，或請求我們提供複製本。但我們依法得酌收必要的成本費用。
- 您有權向我們補充或更正您的個人資料
- 當本契約終止或解除後，或您認為我們不再需要您的個人資料時，您有權請求我們刪除、停止處理或利用您的個人資料。但我們因執行業務所必須（例如法令已規定保存期限），或另外取得您的書面同意時，仍得保存或繼續處理、利用您的個人資料。
- 如您認為我們違法蒐集、處理或利用您的個人資料時，您有權請求我們刪除、停止蒐集、處理或利用您的個人資料。但我們會檢視是否有違法情形，並回覆您結果。
- 如您不願再收到我們的行銷資訊，您有權通知我們拒絕接受行銷。
- 如您要行使上述各項權利，請洽……（註：請補充客戶行使權利之方式、管道）。

6. 您若不提供個人資料的影響

- 如您未正確、完整填寫或提供申辦服務所需資料，可能無法申辦本服務，或將無法即時收到與本服務相關的必要資訊。
- 其他個人資料是您在使用本服務的過程中（自動）產生並記錄，若您不願意我們處理或利用，請依上述權利行使方式辦理。

資料來源：108年通傳事業導入隱私保護管理機制與資料加值服務之研析委託研究_期末報告-上冊_附件2

附錄七｜個人資料保護與管理稽核檢查表

個人資料保護與管理稽核檢查表			
查核項目	查核內容	查核結果	說明
1.法律責任	1.1 應清楚瞭解，違反個人資料保護法將有可能遭到民事損害賠償、刑事或行政處分的處罰。	□符合 □不符合	
2.投入資源人力	2.1 應配置專責人員或組織及相當資源。	□符合 □不符合	
	2.2 應確實訂定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)，並由負責人或法定代理人簽署。	□符合 □不符合	
	2.3 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(TPIPAS)或國際(BS等)個人資料安全稽核機制之規劃及執行計畫。	□符合 □不符合 □不適用	
3.界定個人資料	3.1 應完整界定個人資料範圍。	□符合 □不符合	
	3.2 應保留盤點紀錄，如盤點清冊。	□符合 □不符合	
4.風險評鑑及管理機制	4.1 應針對含有個資之流程進行風險評鑑。	□符合 □不符合	
	4.2 應保留相關紀錄，如風險評鑑表。	□符合 □不符合	
	4.3 風險評鑑之方式應能有效評估流程中之高低風險。	□符合 □不符合	

個人資料保護與管理稽核檢查表			
查核項目	查核內容	查核結果	說明
4.風險評鑑及管理機制	4.4 針對組織所不能接受之風險，應進行有效之風險處理。	□符合 □不符合	
5.事故之應變、通報及改善機制	5.1 針對個資事故應設有完善之通報、應變及改善機制。	□符合 □不符合	
	5.2 應設計於適當期間內以適當方式及內容通知當事人之程序。	□符合 □不符合	
	5.3 應設置遇有重大個人資料事故時，確實通報主管機關之機制。	□符合 □不符合	
	5.4 機制中應含有防止損害擴大、補救措施及防止類似事件再次發生之要求。	□符合 □不符合	
6.蒐集處理及利用之內部管理程序	6.1 資料蒐集、處理應具備確認符合法定要件之程序，並保留相關紀錄（如審核紀錄）。	□符合 □不符合	
	6.2 蒐集當事人個資應履行告知義務（未履行告知義務時，應符合免告知之情形）。	□符合 □不符合	
	6.3 個人資料之利用，應符合蒐集時特定目的之範圍。	□符合 □不符合	
	6.4 如有原蒐集特定目的外之利用，應符合法定要件。	□符合 □不符合	
	6.5 應符合個資法行銷相關規定(如提供拒絕行銷之方式或保留當事人拒絕行使行銷之處理紀錄)。	□符合 □不符合 □不適用	
	6.6 特定目的消失或期限屆至時，應刪除、銷毀、停止蒐集處理利用個資。如未刪除、銷毀、停止蒐集處理利用個資，應有法定理由。	□符合 □不符合	

個人資料保護與管理稽核檢查表			
查核項目	查核內容	查核結果	說明
6.蒐集處理及利用之內部管理程序	6.7 應於蒐集、處理或利用過程中，確保個人資料之正確性，並就不正確或正確性有爭議之資料，有適當之處置方式。	□符合 □不符合	
7.特種個人資料	7.1 應依個資法規定蒐集、處理或利用特種個人資料(病歷、醫療、健康檢查、基因、犯罪前科、性生活)。	□符合 □不符合 □不適用	
8.當事人權利行使	8.1 應提供當事人權利行使之管道，並建立相關程序確保落實8.2到8.5之要求。	□符合 □不符合	
	8.2 受理當事人權利行使時，應確認為當事人或其代理人身份之相關證明文件。	□符合 □不符合	
	8.3 延長回覆期間時，應將原因以書面通知當事人。	□符合 □不符合	
	8.4 駁回當事人申請時，應具備法定要件，並以書面將拒絕事由告知當事人。	□符合 □不符合	
	8.5 應將當事人權利行使回覆情形做成紀錄供機關備查。	□符合 □不符合	
9.個人資料業務委外	9.1 如有委託第三方蒐集、處理或利用個人資料，應對受託方為適當之監督，並保留必要之紀錄。	□符合 □不符合	
	9.2 應於委託契約或相關文件中，約定個人資料委外監督之事項。	□符合 □不符合 □不適用	

個人資料保護與管理稽核檢查表			
查核項目	查核內容	查核結果	說明
10.國際傳輸	10.1 應符合個資法及主管機關關於國際傳輸相關法令之限制。	□符合 □不符合 □不適用	
11.資訊安全（如組織已通過資安相關驗證（如ISO27001）得提供驗證相關紀錄作為本問項之符合證明）	11.1 應針對含有個人資料之檔案設有存取控制措施，包括存取權限設定程序(含存取必要性與最小性之要求)、權限審核、權限清查、存取紀錄留存等。	□符合 □不符合	
	11.2 應針對含有個人資料之檔案進行必要之加密，包括加密要求之規則、方式與強度。	□符合 □不符合	
	11.3 應針對個人資料電子檔案之傳送進行管控，包括使用強度足夠之加密通訊協定、傳送必要性確認等。	□符合 □不符合	
	11.4 應使用合法且無明顯漏洞之軟體，包括系統軟體licence確認、系統軟體即時更新確認等。	□符合 □不符合	
	11.5 應確認必要防毒軟硬體之布建與更新狀況。	□符合 □不符合	
	11.6 應要求處理個人資料之員工或供應商等簽署保密協定。	□符合 □不符合	
	11.7 應針對重要之設備或場域進行必要之管控，包括建立必要安全網路架構、定期進行設備、系統元件、資料庫系統及軟體漏洞修補及可攜式儲存媒體使用安全管理作業規定等。	□符合 □不符合	

個人資料保護與管理稽核檢查表			
查核項目	查核內容	查核結果	說明
11.資訊安全（如組織已通過資安相關驗證（如ISO27001）得提供驗證相關紀錄作為本問項之符合證明）	11.8 人員進出（管理）情形應具體掌控，包括人員存取權限與紀錄、門禁機制與紀錄等。	□符合 □不符合	
	11.9 應保留稽核紀錄。	□符合 □不符合	
12.認知宣導及教育訓練	12.1 應定期針對新進人員及內部員工進行個資保護與管理相關認知宣導與教育訓練，並保留相關紀錄。	□符合 □不符合	
13.稽核機制	13.1 應定期實施稽核，並保留相關紀錄。	□符合 □不符合	
14.紀錄保存	14.1 應保存個資管理紀錄、軌跡資料及相關紀錄。	□符合 □不符合	
15.個人資料安全維護之整體持續改善	15.1 應針對稽核之結果、法規之變更、主管機關或業主之要求等情形定期檢視，並改善公司個人資料保護與管理制度之作法。	□符合 □不符合	
備註	1. 建議事項		
	2. 觀察事項		
	3. 優良事項		

查核結果說明表

項目		定義
查核結果	符合	對本問項有完善落實，並能提具相關佐證證明或說明
	不符合（高風險）	對本問項內容尚未執行、未確實落實以致有違法重大風險
	不適用	無執行與本問項有關之流程或業務，或未達法規適用門檻
備註	建議事項（低風險）	針對查核項目之相關建議
	觀察事項（中風險）	針對查核項目發現可能有負面影響，目前評為符合但未來若未改進則可能視為不符合
	優良事項	針對查核項目發現表現良好之具體事項

資料來源：本手冊自行繪製

主要參考資料

- 個人資料保護法
- 個人資料保護法施行細則
- 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
- 台灣個人資料保護與管理制度（TPIPAS）
- 國家標準 CNS 29100
- 財團法人資訊工業策進會科技法律研究所，《個資保護2.0》，書泉（2019）

國家通訊傳播委員會
NATIONAL COMMUNICATIONS COMMISSION

財團法人資訊工業策進會
INSTITUTE FOR INFORMATION INDUSTRY

stli 科技法律研究所
SCIENCE & TECHNOLOGY LAW INSTITUTE

Personal Data Protection and Management in the Communication Industry