中華民國經濟部
Ministry of Economic Affairs, R.O.C.

經濟部商業司 廣告

臺灣個人資料保護與管理制度
Taiwan Personal Information Protection and Administration System

企業實作案例精選

2016年11月版

目錄

圖目錄

表目錄

壹、緒論

按我國自 2010 (民國 99) 年 5 月 26 日公布個人資料保護法 (以下簡稱個資法) 全文 56 條，並於 2012 年 10 月 1 日施行，取代 1995 年所訂定之「電腦處理個人資料保護法」，個人資料(以下或簡稱個資) 保護與管理已邁入新紀元。歷經 3 年多的實踐，當國內各公務機關或非公務機關逐漸熟悉法令規範時，個資法又於 2015 年 12 月 30 日進行修正，並在 2016 年 3 月 15 日施行。

為協助企業有效因應個資法之要求，早在 2012 年 10 月 1 日個資法正式施行前，在經濟部商業司指導下，財團法人資訊工業策進會科技法律研究所 (資策會科法所) 建置並推動國內唯一以我國個資法為基礎設計之管理制度 - 「臺灣個人資料保護與管理制度」(Taiwan Personal Information Protection and Administration System, TPIPAS)。

表 1 資安及個資管理制度差異概述

資安管理制度	個資管理制度
ISO 27001 (ISO 國際組織標準) 針對資訊安全之管理制度	ISO 29100 (ISO 國際組織標準) 資訊安全技術 - 隱私框架
	BS 10012 (英國標準) 針對個資管理及隱私權維護
	TPIPAS (國內唯一) 以我國個資法為基礎設計之個人資料保護與管理制度

資料來源：TPIPAS制度維運機構整理

此制度推動迄至 2016 年 9 月間，已有近 20 家國內知名廠商從企業內部自發性地要求導入 TPIPAS 制度，如統一超商、全家便利商店、雅虎（Yahoo）資訊、特力屋、康迅（Payeasy）、統一資訊、統正開發（夢時代購物中心）、集保結算所、聯徵中心、訊聯生物科技等優質企業，並通過具公信力之外部驗證，及取得「資料隱私保護標章（Data Privacy Protection Mark, dp.mark）」，將此制度及標章視為企業內部完善個資保護環境之重要工具。

貳、企業建置個資管理制度應注意內容

為落實個資法，及強化企業或組織所擁有之個資保護與管理，實務上我國廠商多透過提供必要資源、建立管理制度或訂定 SOP，確保符合相關法令要求，如建置個資管理制度等。復依我國個資法第 27 條及個資法施行細則第 12 條規定，基於防止個資被竊取、竄改、毀損、滅失或洩漏，目前個資法對於公務機關或非公務機關要求需有整體之安全措施，其具體內容包含配置管理之人員及相關資源，界定個資範圍，個資風險評估及管理機制，事故預防、通報及應變機制，個資蒐集、處理及利用之內部管理程序等 11 大事項，且相關措施內容與企業或組織所欲達成個資保護目的之間，需有適當比例為原則等。

表 2 個資法要求與TPIPAS規範比較表

個資法要求	TPIPAS規範
一、成立管理組織，配置相當資源	Clause 4.4.4 / 4.4.5 / 5
二、界定個人資料之範圍	Clause 4.4.2
三、個人資料之風險評估及管理機制	Clause 4.4.3
四、事故之預防、通報及應變機制	Clause 4.4.6
五、個人資料蒐集、處理及利用之內部管理程序	Clause 4.3 / 4.4.5 / 4.5
六、資料安全管理及人員管理	Clause 4.5.3.2 / 4.5.3.3
七、認知宣導及教育訓練	Clause 4.2 / 4.6.1~4.6.4
八、設備安全管理	Clause 4.5.3.2
九、資料安全稽核機制	Clause 8
十、必要之使用紀錄、軌跡資料及證據之保存	Clause 7.3
十一、個人資料安全維護之整體持續改善	Clause 9

資料來源：TPIPAS制度維運機構整理

為符前述法令要求事項，並經執行團隊綜整歷年取得 dp.mark 標章組織之經驗（註：以下本文提及之廠商皆已匿名化，且相關經驗或範/案例內容等業經改寫），擬以實作角度出發，研提我國企業或組織建置個資管理制度應注意事項。以導入廠商經驗為例，選擇 TPIPAS 作為符合我國個資法規範之首選，其主要係因坊間個資、資安相關管理系統眾多，如前述 BS 10012 針對個資管理及隱私權維護、ISO 27001 針對資訊安全管理系統。然公司內部需求以個資保護與管理為主，最終選擇 TPIPAS 係因 BS 10012 為英國標準，所引用之條文與我國個資法不盡相同，且其為民間組織較不若經濟部主導之 TPIPAS 較具公信力。

因此，本文所述具體內容皆以個資法及相關法令，並援引 TPIPAS 規範及其在個資法落實之狀況(尤其是個資法第 27 條及同法施行細則第 12 條)為主，另搭配實務案例，供作建置個資管理制度之實作參考，希冀協助我國企業或組織瞭解個資保護與管理制度之重要內容。綜上，本文試先分述應注意要項，並依實際導入 TPIPAS 廠商之經驗進行分享或說明如後。

一、配置管理之人員及相當資源

(一)、建置管理制度應注意事項

無論是公務機關或非公務機關，凡是有意建置內部個資保護與管理制度之組織，其業務推動等都必須仰賴實際執行之人員。因此，首要任務係指派相關專責人員，並提供必要之資源。一般而言，在人員配置部分，除依組織人數、規模，並考量單位層級、功能、業務屬性等因素，主要可能包含 1.管理代表，以確保必要資源投入，及監督管理制度之執行，且應取得充分授權，可以跨部門溝通、協調；2.實際執行之管理或種子人員，從事個資蒐集、處理及利用等具體業務；以及 3.檢視之內稽或內部評量人員，以協助管理制度之運作。

表 3 內部管理制度推動人員事例

類別	說明
1.管理代表	建議由最高管理階層或指定一定層級人員擔任。且本項人員應確保必要資源投入，及監督管理制度之執行，且應取得充分授權，可以跨部門溝通、協調。
2.執行人員	組織內部涉個資業務相關部門皆需派員，如人資、IT、法務、行銷、業務等，屬實際執行個資管理制度或種子人員，且可考量取得TPIPAS管理師資格。
3.內評或稽核人員	協助內部評量或內稽，可由稽核室或曾具稽核其他管理系統經驗之人員，如ISO 9001品質管理系統等，並可考量取得TPIPAS內評師資格。

資料來源：TPIPAS制度維運機構整理

至於必要資源之投入，係確保制度建置非單純之宣示或口號，而有配合之人、物力或相關資源，如財務支援。尤其是管理代表，更應善盡監督之責，除協助整合、溝通外，也應確保所需之資源，使管理制度運作順利。

此外，企業或組織所投入之資源，應包含有形及無形內容，其中有形部分如前述人、物力、設施或設備等。另無形部分更應重視，由於個資法施行後，對於組織於業務範圍內，或相關營運行為等，有意蒐集、處理、利用個資時，除有一定認知外，即應規劃符合法規之安全維護措施，或甚至建置內部完整個資管理制度，並強化宣導及教育訓練等，切莫存有僥倖心態，或輕忽個資相關法令之要求，以避免事故發生後得不償失。

(二)、企業實作參考

在人力配置上，除配合組織人數、規模，並考量單位層級、功能、業務屬性等，以功能面為例，如具體可由客服部門協助當事人權利行使之相關業務、資訊(IT)部門提供系統支援、法務部門協助檢視相關法令或契約之內容，以符個資法要求。

在以往導入經驗上，如某 A 公司係採內外部共同協助之方式，內部先分為三個小組，如風險管理小組、制度文件建置小組、內部稽核小組，從管理政策至員工教育訓練相關程序文件，分由三個小組負責撰寫。此外，在外部協助是委請專業機構提供協助諮詢顧問服務，該專案計畫涵蓋：該公司及受任機構團隊，專案會議、個資資產盤點，風險評鑑、安全管控措施，建立程序文件、教育訓練，內部稽核及外部稽核驗證等項目。

另組織可依前述建議自行組成團隊並規劃、執行相關制度，或可考量委請專業輔導機構協助建立內部個人資料保護與管理制度。此外，從實際建置經驗來看，尚建議：1.各部窗口適時應採取輪調制，以充實管理人力。及 2.由資深同仁帶領資淺同仁一併參與內部訓練課程，以確保代理人力。

而資源之投入尚可表現在對於管理制度推動人員之獎勵面與績效考核面，除對於管理制度推動有功之人員從優敘獎外，部分公司會將管理制度之推動亦列入年度績效考評之一環，亦即將個資保護納入工作項目內，而非額外增加管理人員之工作負擔。

二、界定個人資料之範圍

(一)、建置管理制度應注意事項

對於企業或組織要確認內部管理制度是否符合個資法之要求時，界定個人資料之範圍（可先參照個資法第2條對個人資料之定義，及是否屬第 51 條之例外規定），或進行所謂「個資盤點」為首要工作之一。此一作業之目的，在於瞭解企業或組織所保有之個人資料（指以公司為蒐集主體），其是否合法蒐集（如是否已先履行個資法第8條或第9條之告知義務，及第15、19條關於蒐集或處理之規定）、利用（如個資法第16、20條關於利用之規定），評估相關風險，及供企業內部規劃所需之管理措施等（個資風險評估及管理機制相關內容另如後述）。

由於進行個資盤點的目的在於確認個資管理範圍，及蒐集、處理或利用之適法性；及進行風險評估及因應等。個資盤點可協助組織瞭解內部保有個資之狀況，然盤點需先界定個人資料之範圍。其主要執行方式可能有二：一是透過內部之作業流程，依個資生命週期（如蒐集、處理、利用、銷毀）進行判斷，如檢視加入會員（實體或網站）之流程，是否會先要求消費者提供個資（如姓名、電話、地址等）、及提供後公司會進行行銷或其他利用行為，或如何對消費者提供客戶服務；另一是直接整理各部門所存有之文件、檔案等，如各類申請表（紙本或線上之會員或服務申請表）、協議書或契約、單據或類似文件，以確認有無個資相關內容。

一般來說，進行前述盤點作業完成後，企業或組織尚會將保有之個資填入個資盤點表或盤點清冊內，該表單主要欄位計有：作業流名稱、個人資料種類、直接/間接蒐集、告知義務、委託/受託、儲存（含資料載體、保管場所、保管期限）、及數量等。惟組織可自

行依據實際需求，調整表格具體內容（如下表），並可透過紙本或系統協助進行相關作業。

表 4 個人資料盤點表範例

編號	個人資料檔案名稱	個人資料種類	直接蒐集	間接蒐集	告知 Y/N	委託 Y/N	儲存	（其他待補）
								實際欄位可視公司需求增補

資料來源：TPIPAS制度維運機構整理

(二)、企業實作參考

如前所述，個資盤點主要執行方式略分為：1.透過內部之作業流程，依個資生命週期（如蒐集、處理、利用、銷毀）進行判斷；或 2.直接整理各部門所存有之文件、檔案等，以確認有無個資相關內容。相關流程或待盤點文件之判斷依據尚可以 1.公司營業項目，如營業項目所跨及之領域、公司性質可能牽涉的主管機關及法規；或 2.公司作業流程，如公司現有作業流程的初步判斷；或 3.公司重要業務，如營運、獲利、客戶...等業務，進行綜合判斷。

以某 B 公司為例，該公司進行盤點的過程，首先是 1.先確定權責單位（人員，負責盤點作業、彙集等，另由法務或 IT 部門...）；再依序為 2.確定個資盤點清冊格式欄位內容，如特定目的、符合法定之情形、法源依據、直接或間接取得、保管場所、儲存方式、外部利用單位、特定目的外之利用符合情形、刪除銷毀方式；嗣為 3.確定個資盤點原則，如同一作業產生不同名稱之紙本文件是否整併、

不留存之紙本文件或光碟磁片媒體是否盤點、資訊單位資料庫是否盤點等；最後是 4.確定個資盤點清冊更新週期。

此外，在實際操作上，尚建議組織內部應訂定盤點表單欄位填寫說明，及強化教育訓練（如後述說明內容），確保同仁認知之一致性，如直接/間接蒐集之定義、法令依據等。此外，內部完成表單初稿後，建議宜指定人員（如各單位種子人員或推行小組成員），協助彙整及確認，以確保盤點作業能符合內部規範等要求。

而根據執行 TPIPAS 驗證之經驗，企業在個資盤點之過程中，通常需要解決之問題如：疏忽部分的個資檔案未納入盤點清冊、對於盤點清冊之填寫方式有不一致或認知錯誤之情形。因此，企業為解決此兩種問題，常會採用以下方式：

方式 1 - 繪製個資作業流程圖：參加盤點作業之不同部門，將其日常作業過程中所接觸到之個資，以流程圖之方式呈現，即由何人或何部門蒐集或接收到此筆個資，後續又會傳輸到何部門或如何利用。在不同部門之間，可透過流程勾稽之方式，提升盤點之完整性，並減少漏盤之問題。

方式 2 - 製作清楚之個資盤點範例與說明：為使不同參加之部門均能輕易理解盤點清冊如何填寫，製作清楚之個資盤點範例與說明，是較佳之方式。另外，如參加個資管理制度之人員有異動或交接之情形時，配合個資內部之教育訓練，提供內部人員如何填寫盤點清冊之說明，亦屬可行之作法。

三、個人資料之風險評估及管理機制

(一)、建置管理制度應注意事項

進行完個資盤點之作業後，企業或組織已大致瞭解內部保有之個資概況（如個資類別、數量、保有部門、期間或管理方式），及可能涉及之業務或流程等，再來即可針對相關個資進行風險評估及制定後續管理措施。而所謂風險（risk）除實際管理上可能遭遇被竊取、竄改、毀損、滅失或洩漏之情形外，也包含法令要求，如違反個資法相關規定，可能產生訴訟或被主管機關裁罰等。

此外，個資類別或數量多寡等，並不當然等同於風險高低，企業或組織必須先進行風險分析及評估，如透過瞭解所保有的個資內容或價值，以掌握個資被竊取、竄改、毀損、滅失或洩漏等可能對公司帶來的影響、及事故發生時所能承受或可能造成的損失，俾利規劃所採行適當的措施或管理機制。

承上，常見的風險分析流程，包含判斷風險的種類、確認風險產生的原因、評估風險可能的衝擊，及提出相關的因應對策。尤其企業或組織在研提風險因應對策時，還會考量該風險之發生機率、損害程度，俾判斷採取轉嫁、避免、接受或控制（如下圖）。

資料來源：TPIPAS制度維運機構整理

圖 1 風險因應對策概述

企業或組織進行風險評估時，可先由各部門自行提出初步建議，針對個資檔案之類型（屬實體紙本或系統資訊）、弱點或威脅（如未符相關法令要求、人員認知不足、內部管理不善）、可能發生機率或頻率等，並可進一步區分機密性、完整性、可用性、或個資價值等，制定適當措施內容，例如：IT 部門對於載有重要個資檔案之伺服器，因一旦發生相關事故時，恐對組織產生不利影響，故須採取較嚴格之管理措施，如採取登入權限控管，進出機房搭配門禁管制等。

此外，為免同仁認知不一致，使風險評估結果落差過大，或意圖降低風險值以規避管理要求，除強化宣導及教育訓練外，內部仍宜由種子成員、一定層級之管理職人員或甚至管理代表，針對整體風險評估及對應所採取的管理機制，進行最終確認或定期檢視，以確保管理機制能符合需求。

(二)、企業實作參考

以某 C 公司為例，該公司個資風險之分析進行方式包含：1.確定權責單位，2.確定個資價值衝擊判定等級、威脅或弱點判定等級表、威脅弱點風險組合，3.確定可接受風險值之基準值，4.確定風險安控計畫格式、內容、負責部門及完成期限，以及 5.確定風險評鑑清冊更新週期（半年或一年）。

而具體分析風險的做法，即可依據蒐集、處理、利用的流程，建立符合企業自身專屬之風險事件清冊如下表：

表 5 個資風險事件清冊表範例

資料型態	處理情境	具體風險類型	風險對策
電子檔	蒐集	網站設計存在弱點被不當存取	採取防範 SQL injection 攻擊對策
	處理	業管人員個人電腦帳號、密碼管理不確實，遭無權限人員不當存取	處理權限設定、防範登錄帳號密碼被他人知悉
	利用	業管人員將個人資料使用於特定目的外之利用	部門主管指導監督業管人員
紙本檔	蒐集	領取作業不確實致遺失	取得領取記錄，將領取的紙本收至同一文件夾內
	處理	資料放置於桌上後遺失遭外部人員外洩	保持桌面淨空
	利用	傳送過程中遺失	確實登錄傳送程序，如公文掛號或簽收簿

資料來源：TPIPAS制度維運機構整理

四、事故之預防、通報及應變機制

(一)、建置管理制度應注意事項

縱使已針對個資進行盤點，並進行風險評估及採取適當之管理機制等，但由於現代科技日新月異、或相關管理措施仍可能有偶發之疏漏發生，因此，企業或組織對於事故仍須有正確之認知：不可能百分之百避免，但除平時落實執行內部個資管理制度外，並要確保事故發生時，能採取適當之對應措施，如啟動應變機制、通知當事人、通報相關機關，將可能之影響或損害（如訴訟費用、行政裁罰、或甚至是商譽）降到最低。

如前所述，在個資管理制度內，可能之風險包含個資被竊取、竄改、毀損、滅失或洩漏等情形。為降低風險，及控制風險實現（此時即可稱為事故）時之損害，企業或組織對於個資事故之預防、通報及應變，應有對應之措施。一般來說，因應措施採取之時點可略分為事前、事中、事後三階段且重點有所不同，其中 1.事前著重於透過前述風險評估之結果，採取對應之預防措施。而 2.事中在於即時反應，減少事故發生當時所造成之損害，並依個資法第 12 條之規定，查明事故發生原因（根因），及通知個資當事人等。至於 3.事後管理重點在於有效解決根因發生之緣由、及避免事故再次發生，則可搭配內部改善措施等。

(二)、企業實作參考

組織內部針對事故預防、通報及應變之機制，可能包含：應變計畫、通報程序、分級處置、應變程序、教育訓練及監控措施等內容。例如：公司可成立應變小組，由管理代表或一定層級之主管擔任小組組長，負責事故應變之監督、管理、協調及相關報告。至於

其他業務部門主管或代表，負責協助執行應變機制，並及時通報小組成員。另由媒體聯絡人或公關單位處理公共關係等。

此外，倘不幸發生事故後，企業或組織除在網站或實體店面進行公告外，由於個資法第 12 條規範主要係針對特定當事人，其通知之重點內容包含：1.對當事人部分（如會員、消費者等個資遭外洩對象），應說明事故發生原因、提供之諮詢管道、協助方式；而通知之方式，依個資法施行細則第 22 條規定，無論是言詞、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皆可。及 2.組織內部採取之作為，如啟動前述應變機制，採取對應之處理方式，如系統處置/權限調整、自行或委外進行數位鑑識等。且事故發生後，建議企業或組織宜延長客服時間或規劃非營業時間之協助方式，以確保個資當事人之權益。

表 6 通知當事人內容範例

非常抱歉，因 OO 緣故造成台端個資外洩（如有需要，可再進一步說明含事故發生之時間區間、受影響個資範圍…等資訊），任何自稱本公司客服或某A銀行人員等，要求台端操作帳務事宜係詐騙行為，請勿聽信，並儘速與本公司聯繫，專線電話為…

某 X 公司，2016 年 9 月 Y 日

Logo/ 官網

資料來源：TPIPAS制度維運機構整理

另，除個資法要求及 TPIPAS 條文規範（如後述）外，依資料隱私保護標章 dp.mark 管理要點之 6.1 組織報告義務：發生事故時，組織應即通知制度維運機構，並於查明後，盡速向制度維運機構提出書面報告，說明事故之原因、損害狀況及處理之情形。及 6.2 制度維運機構協助：必要時制度維運機構得派員協助組織查明事故。有取得該標章之廠商亦需注意相關規範。

表 7 TPIPAS規範對事故通報等規範

條號	TPIPAS條文重點
4.3 個人資料保護管理手冊	(前略)具體規則內容至少包括： (5)事故緊急應變
4.4.6 事故之緊急應變	為避免事故可能產生之不利益及影響，組織應訂定事故緊急應變措施。相關措施應至少包括： (1)查明後以適當方式通知當事人事故發生，並提供後續查詢與處理管道。 (2)防止組織所受損害擴大之方法。 (3)避免類似事件再次發生之方法。 (4)將事故通報授證機關。

資料來源：TPIPAS制度維運機構整理

五、個人資料蒐集、處理及利用之內部管理程序

(一)、建置管理制度應注意事項

經整理個資法相關規範，我國企業或組織在蒐集、處理及利用應有的管理程序主要包含以下內容：

表 8 個資法對個資蒐集/處理/利用等管理程序之整理

規範要項	個資法條文
1.個人資料蒐集應注意之事項及告知義務之履行	第 15、19 條 第 8、9 條
2.確保於特定目的內利用個人資料及特定目的外利用時為合法	第 16、20 條
3.利用個人行銷之程序	第 20 條
4.蒐集、處理及利用特種個人資料之程序	第 6 條
5.因應限制國際傳輸個人資料之程序	第 21 條
6.委外監督程序	第 4 條
7.提供當事人行使權利之程序	第 10,13 條
8.確認個人資料正確性之程序	第 11 條
9.保有個人資料之特定目的消失或期限屆滿之程序	第 11 條

資料來源：TPIPAS制度維運機構整理

此外，相關蒐集、處理及利用程序亦應配合法令修正適時更新，以 2016 年 3 月施行之個資法為例，在本次個資法修正前，企業或組織要取得個資當事人之同意，係以書面同意為主。基此，在以往流程或系統的設計上，只要能確定該書面之形式，或採用符合電子簽章法之電子文件即可。但在修法後，對於一般個資之蒐集、處理及利用，於表示同意時，已無書面之要求，又因修正後之個資法課予蒐集者對個資當事人同意之事實，應負舉證責任。為避免日後不

必要之困擾，建議我國企業或組織應考量建立內部一致性處理流程，或納入系統既有作業內容，如增加作業流程內之節點（checkpoint），確保個資蒐集、處理或利用相關程序已標準化，並適度留下相關紀錄，始可能符合法規之需求。

(二)、企業實作參考

如前所述，個資法對個資蒐集/處理/利用等管理程序應包含說明：(1)個人資料蒐集應注意之事項及告知義務之履行，(2)確保於特定目的內利用個人資料及特定目的外利用時為合法，(3)利用個人行銷之程序，(4)蒐集、處理及利用特種個人資料之程序，(5)因應限制國際傳輸個人資料之程序，(6)委外監督程序，(7)提供當事人行使權利之程序，(8)確認個人資料正確性之程序，及(9)保有個人資料之特定目的消失或期限屆滿之程序等內容。考量實務運作主要需求，茲摘陳說明告知義務、特定目的利用、委外監督及當事人權利行使等重點如下：

1.個人資料蒐集應注意之事項及告知義務之履行

以非公務機關履行告知義務之可能內容為例，除個資法第 8、9 條之要求項目外，如：(1)公務機關或非公務機關名稱，(2)蒐集之目的，(3)個人資料之類別，(4)個人資料利用之期間、地區、對象及方式，(5)當事人依第三條規定得行使之權利及方式，及(6)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。並應確認有例外無須告知之情形，及依據組織對於個資蒐集情況（實體、網路）採取適當之告知方式。

表 9 個資法對直接/間接蒐集告知義務之要項

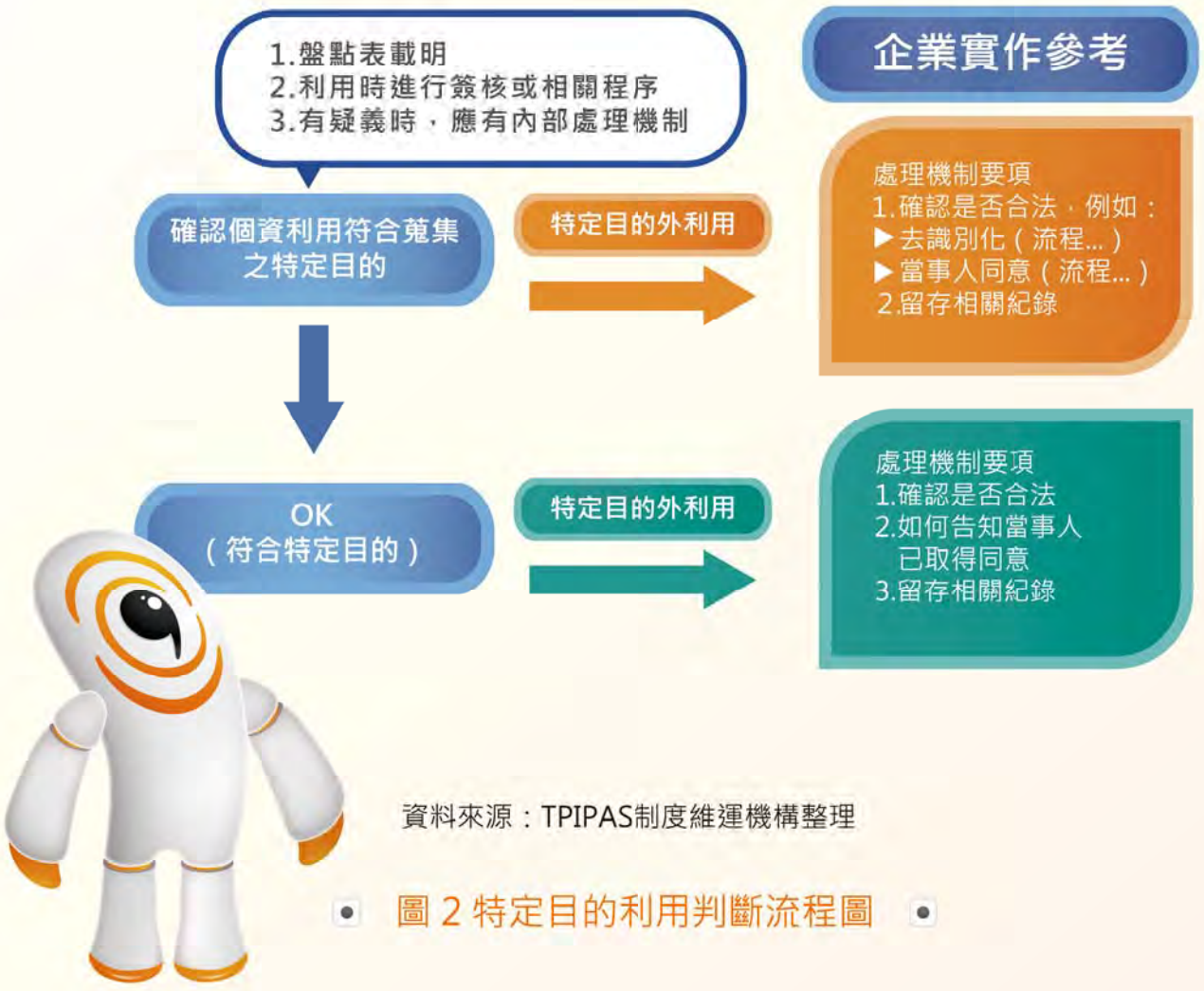
	直接蒐集時之告知義務	間接蒐集時之告知義務
法源依據	個資法§ 8	個資法§ 9
告知時機	蒐集時	1.處理或利用前 2.首次對當事人為利用時
告知內容	1.蒐集機關名稱 2.蒐集目的 3.個資類別 4.利用地區、期間對象與方式 5.當事人權利行使之方式 6.得自由提供時，不提供對當事人權益之影響	1.蒐集機關名稱 2.蒐集目的 3.個資類別 4.利用地區、期間對象與方式 5.當事人權利行使之方式 6.間接蒐集時之資料來源
例外規定	1.法律規定得免告知 2.係機關執行法定職務或履行法定義務所必要 3.告知將妨害法定職務執行 4.告知將妨害公共利益 5.當事人明知應告知之內容 6.蒐集非基於營利之目的且對當事人無不利影響	1.有左列情形 2.當事人自行公開或已合法公開之個資 3.不能向當事人或其法定代理人為告知 4.基於公共利益為統計或學術研究之目的而有必要等 5.大眾傳播業者基於新聞報導之公益目的而蒐集個資

資料來源：TPIPAS制度維運機構整理

承上，組織首先要確認有例外無須告知之情形；並區分資料蒐集情況（如實體、網路）採取適當告知方式。至於實際導入廠商之運作經驗，除透過網頁上告知外，亦會配合載具科技或用戶使用習慣，提供 e-mail 或 QR code 等方式供消費者查閱。

2.確保於特定目的內利用個人資料及特定目的外利用時為合法

在個資管理實務上，亦非常在意確保於特定目的內利用個人資料及特定目的外利用時為合法，因為原則上是不允許為特定目的外之利用，但運作實務上常需透過 SOP 或簽核等程序，以協助內部成員進行判斷。茲以下圖為例，說明一般企業或組織針對特定目的進行判斷之可能方式：



資料來源：TPIPAS制度維運機構整理

圖 2 特定目的利用判斷流程圖

3.委外監督程序

有鑒於我國企業或組織基於人力、成本、專業等考量，將部分業務委外處理，已屬常態。但委外業務如果涉及個人資料，依個資法第 4 條之規定，被委託者（受託者）在蒐集、處理或利用個人資料之範圍內，視同委託機關。

為符個資法對於委外監督管理之具體要求，建議組織或可透過契約約定，或進行實地查核等方式為之。如以契約約定為例，常見約定內容為：(1)乙方在執行業務所必須之範圍內，應依「個人資料保護法」第 27 條規定採行「個人資料保護法施行細則」第 12 條所規定之安全管理措施，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。或(2)乙方僅得於甲方以下指示之範圍內，蒐集、處理或利用個人資料：預定蒐集、處理或利用個人資料之範圍、類別、特定目的...。更甚組織亦可要求委外廠商取得dp.mark，以強化委外監督管理力度。

至於實地查核方式，可能包含：(1)定期執行/配合相關稽核規劃、(2)配合集團統一作業或依客戶要求、(3)不定期抽查。而委託方亦可直接前往受委託方進行檢視；或由受委託方自評（由委託方提供表單）完後，委託方再行前往。

4.提供當事人行使權利之程序

由於個資法兼具避免當事人人格權受侵害及促進個人資料之合理利用，故針對當事人權利行使亦為管理重點之一，組織需注意個資法第 13 條 15 或 30 天期限之規定。以及第 10 條規定之例外情形，包含：

(1)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。(2)妨害公務機關執行法定職務。(3)妨害該蒐集機關或第三人之重大利益。

表 10 個資法對當事人權利行使之規範要項

事由	原則	例外
個人資料正確性有誤	無爭議：應主動或依當事人之請求補充或更正	無
	有爭議：應停止處理或利用該個人資料	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	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	同上
違法蒐集、處理、利用	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	無
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	無
違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害	查明後以適當方式通知當事人	無

資料來源：TPIPAS制度維運機構整理

而實務運作上，當事人權利行使管理重點包含：(1)有無對外之受理窗口；(2)具體作業程序，如專責人員或單位、管理代表功能；(3)內部定期報告，如配合相關統計分析，或利用管理審查或其他會議，讓最高管理階層或管理代表掌握相關資訊。

六、資料安全管理及人員管理

(一)、建置管理制度應注意事項

隨著現代科技的進步，個資常伴隨儲存媒體或載體（如紙本、電子檔案）之不同，而有諸多保存形式，也因此成為內部擬定管理機制時，所需併同考量的內容。基於此，在資料安全及人員管理方面，個資檔案、載體、保管場所之管理與其如何避免遭入侵、竊取、遺失等事故發生，以及一般、權責人員權限如何分配、控管，且不造成實際業務執行困擾等，都是管理機制所應考慮的重點。

為確保企業或組織所保有個資之安全，可先確認內部相關個資之內容、數量、管理人員、保管場所狀況、該個資對當事人權益之重要性等，俾搭配可能的管理作為。例如使用儲存媒體時，應要求管理人員妥善保管，並訂定必要之使用規範，如權限控管、留存操作紀錄，避免個資被竊取、竄改、毀損、滅失或洩漏。

而人員管理除制定相關操作規範，確保作業流程或程序一致外，亦可結合員工管理措施(如工作規則、聘僱契約)，或簽署保密條款，並定期進行教育訓練等，以確保從業人員確實瞭解組織內部之個資保護與管理規定。

(二)、企業實作參考

以某 D 公司為例，導入 TPIPAS 之目的，在於建立並落實施行個資及資訊安全管理，提昇該公司相關人員持續改善個資及資訊安全管理之能力。該公司體認到個資管理的重要性，為因應外部環境與資訊，將個資及核心業務流程，視為公司重要資產，透過日常作業及持續改進，例如：審視日常作業流程、建立網購平台之開發維運、資訊基礎建設等個資及資訊安全要求，制定相關資料安全及人員管理措施，如權限控管、依 SOP 進行個資蒐集、處理、利用，以維持保護會員及員工個人資料安全之可信賴度，並配合法令政策、內部標竿學習方式，逐漸建立提昇認知，強化內部整合。

七、 認知宣導及教育訓練

(一)、建置管理制度應注意事項

如前所述，凡企業或組織相關業務或營運行為，有蒐集、處理或利用個資時，內部規範或管理制度即應符合個資相關法令之要求，故組織如何建立正確之認知，及透過宣導或教育訓練，讓管理階層或全體員工對瞭解個資法、主管機關要求及內部規範內容、SOP 等，以確保符合相關法令，實為重要之工作。

除個資法第 27 條及施行細則第 12 條對安全維護措施之 11 大項介紹，已陸續於本文相關內容陳述外，另依 TPIPAS 規範要求組織應確保其人員對個人資料管理具體正確的認知及能力，如個資法概述、個資盤點、風險評估等。而可能訓練對象尚包含：一般人員、權責人員（如推行小組成員），且須建立紀錄與改善機制。

表 11 內部個資教育訓練可能對象及內容

對象	可能訓練內容
一般人員	基本教育訓練，如個資法概述、組織個資管理相關規定...
權責人員	符合必要能力需求，如取得 TPIPAS 專業人員資格，或個資管理實務等課程，如個資盤點、風險評估、委外監督管理、事故應變...

資料來源：TPIPAS制度維運機構整理

此外，企業或組織對於個資管理之政策、目標及相關作業規範等亦為內部宣導及教育訓練之重點。由於個資保護係組織全體應關切之內容，故前述認知宣導及教育訓練的對象為工作上可能涉及個資之所有員工，含正式、派遣員工或臨時人員。而宣導或訓練項目，除配合組織政策、目標之調整，亦須配合個別員工業務內容，施以

必要之訓練內容，且建議應確保訓練之有效性（如測驗、心得分享、問卷調查）及留存必要之紀錄等。

(二)、企業實作參考

首先，在提昇認知宣導方面，因坊間個資、資安相關管理系統眾多，如 BS 10012 針對個資管理及隱私權維護、ISO 27001 針對資訊安全管理系統，以某 E 公司為例，該公司需求以個資保護與管理為主，最終選擇 TPIPAS 係因 BSI（英國標準協會）引用之條文與我國個資法不盡相同，且其為民間組織較不若經濟部主導之 TPIPAS 較具公信力。故該公司第 1 階段先辦理教育訓練，第 2 階段為檢討改善涉及個資作業流程，第 3 階段始導入 TPIPAS，以凝聚共識。

再者，企業或組織常透過安排教育訓練，或針對特定作業流程或程序，進行宣導。以某 F 公司為例，該公司製作有個資小卡，分別說明個人資料安全管理組織架構圖、個資事故發生緊急應變流程。

八、設備安全管理

(一)、建置管理制度應注意事項

設備安全管理係以實體之物理環境為主要管理對象，例如辦公區域、機房、IT 設備等。企業或組織應針對不同之作業內容、環境及個資種類相關需求，搭配對應其特性之管理作為，如人員進出重要機房須登記，並有門禁、監視攝影機；機房內有溫濕度監控、消防設備，或採異地備援機制，以因應意外發生之狀況等。

承上，相關設備安全管理尚可區分：紙本（製作、傳遞、儲放）、系統，並配合業務、依據機敏性不同處理，或依專人、專區（還有權限、帳密）等方式進行管理。

(二)、企業實作參考

以某 G 公司為例，該公司確定導入後，即開始著手資源分配與投入，例如：採購密件信封，要求公務個資以外之文件於傳遞過程需裝袋彌封；建立專區專機，除資訊部門、人資部門設置專區，並搭配門禁管制、監視器外，其他部門設置專機，要求涉及機敏個資應於專機操作；購置資訊軟硬體設備，如建立網頁應用系統防火牆及資料外洩防護系統，添購資料庫稽核工具，強化資料庫監控、預警及舉證功能，增加 IP 位址管制設備、遠端連線作業資料安全防護機制、網路傳輸加密機制。

九、資料安全稽核機制

(一)、建置管理制度應注意事項

稽核或內部評量的目的，在於確認企業或組織之個資蒐集、處理或利用行為，及個資管理制度之運作狀況等，是否符合個資相關法令、TPIPAS 規範及內部制度要求。

為確保個資檔案之必要安全措施已被施行，或相關安全維護計畫已落實執行，組織可透過內稽或內部評量等機制確認。此外，執行內部稽核或評量之依據，除個資法等法令規定外，尚包含組織之內部規範，如蒐集、處理及利用之相關程序。且資料安全稽核機制之執行方式或流程可由組織自行決定，包含範圍、頻率、方法，惟建議應至少每年執行 1 次。

又，組織執行此一作業時，可由內部人員自行規劃、執行或委外處理，但重點在於相關人員須具備一定之認知及能力，熟悉法令及內部規範，且有專業證照或資格更佳，如取得 TPIPAS 內評師，或有其他類似管理系統之稽核經驗，如 ISO 27001 資安管理系統。

(二)、企業實作參考

在實際操作上，於執行稽核前常會制定稽核或內評計畫，由稽核部門、小組或稽核員依涉個資之重要業務、作業流程或部門別，分別規劃一定時間，如數小時或一天（且配合組織工作狀況，稽核計畫之執行或可彈性處理，如於一週內完成，或分月、季進行），輔以運用查檢表(checklist)、訪談等方式，通盤檢視相關文件、表單、紀錄，並搭配各部門實地審查，以確認組織整體之個資蒐集、處理或利用等行為，悉符合法令或內部管理制度規範。

如TPIPAS內部評量之規範，會確保組織內部個資保護與管理制度1.符合法規及本制度之要求；及2.符合個人資料保護管理政策、手冊及相關具體規則之要求。另為符合PDCA（Plan、Do、Check、Action）及落實稽核精神，應將內部評量之規劃、執行、報告、改善、追蹤等事項製作書面之內部評量報告並依內部規範進行改善、跟催。

十、使用紀錄、軌跡資料及證據保存

(一)、建置管理制度應注意事項

使用紀錄、軌跡資料及證據保存對於組織內部個資保護或管理制度用途甚廣，例如：可作為內部安全管理措施之一環，如軌跡資料包含相關 log 紀錄，可判別資料存取人員、時間、設備等，搭配內部控制作為或規範，倘發生有異常狀況，即可適時處理。

(二)、企業實作參考

因個資法第 7 條所稱同意之情形，如當事人經蒐集者告知法定事項，表示允許；或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，未表示拒絕，即可推定其同意。且資料蒐集者（如公司）就當事人同意之事實，負舉證責任。故對於實際業務承辦人或公司，如何證明當事人允許或未表示拒絕之意思表示，恐易生爭議。此時，如有相關使用紀錄、軌跡資料及證據保存，亦可協助訴訟程序之舉證。

十一、個人資料安全維護之整體持續改善

(一)、建置管理制度應注意事項

企業或組織可透過建置個資管理制度，符合相關法令需求。然如何建立機制妥處個資管理事宜，非僅由 IT 部門或專業人員一己之力，可思考完善內部管理制度，並由管理代表提供必要資源，且配合各部門相關人員之協助。故管理代表或最高管理階層應定期檢視整體管理措施或制度，並對應改善部分進行跟催。

在持續改善過程中，除關切相關效益外，檢視安全管理措施之項目可包含：1.安全措施之執行狀況，2.內部檢視結果及應改善部分，3.個資相關法令修訂狀況，4.內外部因素變化（如社會情勢、技術發展），5.組織業務領域之調整或變動等，俾賡續精進管理效能。

表 12 TPIPAS對整體個資管理制度持續改善之規範

人員相關	機制相關
5.1 最高管理階層 最高管理階層之責任應包括： (1)決定個資保護管理政策。 (2)決定資源管理。 (3)決定個資保護管理組織架構及權責劃分。 (4)定期檢視管理制度。 (5)建立有效的溝通機制。	9.1 定期檢視 個資管理代表為落實個人資料保護管理，應每年定期召開檢視會議，召集相關權責人員，檢視個人資料保護管理制度，以書面紀錄檢視結果，並報告最高管理階層。 定期檢視會議應檢視下列事項並提出檢視報告： (1)個人資料管理制度執行狀況及其分析。 (2)矯正及預防措施之成效。 (3)有效性量測之結果。 (4)個人資料處理之相關法令以及其他相關規範之修改狀況。 (後略)
5.2 管理代表 最高管理階層應指派管理階層成員之一，擔任個人資料保護制度管理代表，其應有之責任與職權包括： (1)負責維持個人資料管理制度運作之有效性，並建立必要內部人員結構。 (2)確保職務執行過程之公正性與客觀性。 (3)確保個人資料管理制度所需的各項程序被建立、實施與維持。 (4)向最高管理階層報告個人資料管理制度之實施成效與改善措施。	

資料來源：TPIPAS制度維運機構整理

(二)、企業實作參考

以某 H 公司為例，透過 TPIPAS 進行內部資料管理流程之實際效益包含：1.不過度蒐集（必要時遮蔽或去識別化）；2.減少接觸人員（配合權限控管），3.保管場所及方式、資料刪除及銷毀等均有一致性標準，如電子檔案；4.提供資料之內容以必要性為原則；5.保留完整之紀錄；6.程序文件規範明確，較能落實內部稽核之執行；7.有效防範個資外洩事件，降低營運風險。

參、結論

除前述由實際建置個資管理制度之經驗出發，提供我國企業或組織應注意要項內容外，我國企業或組織究該如何執行始能符合個資法相關規範，各部會如中央銀行、內政部、交通部、金管會、勞動部、經濟部、財政部、教育部等，迄今已陸續發布之 20 多項法規命令，如「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法[1]」規範包含非公務機關之個人資料保護之規劃，個人資料之管理程序及措施，個人資料之安全稽核、紀錄保存及持續改善機制等。因此，這些法規命令對於企業或組織落實個資法或相關法令，已可提供具體之參考，如非公務機關應依其業務規模及特性，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等。

我國廠商除依前述參考範例或內容建立安全維護機制外，為確保整體個資業務運作及需求，應適時調整管理制度，甚至可責成專責部門或人員，積極掌握國內外法規動態、法院判決等資訊，並配合營運策略或目標，透過PDCA（Plan、Do、Check、Action）模式建立系統化管理制度，規範個資之蒐集、處理或利用等程序，以符合個資法及其他法令規範。基此，衷心建議我國企業或組織可進一步規劃通過具公信力之外部驗證，如專以我國個資法為設計核心之臺灣個人資料保護與管理制度（TPIPAS）[2]，及取得資料隱私保護標章（dp.mark），以彰顯個資管理效能及避免可能風險。

---

[1] 金管會於 102 年 11 月 8 日發布、105 年 5 月 5 日修正。

[2] 具體介紹請見李沛宸，〈機關必備個資保護與管理工具 - 簡介「臺灣個人資料保護與管理制度」〉，《集保結算所雙月刊》，第 219 期，頁 13 至 23（2015）。

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

科技法律研究所
SCIENCE & TECHNOLOGY LAW INSTITUTE

106 台北市敦化南路二段 216 號 22 樓
22 F. No. 216, Sec. 2 Dunhua S. Rd. Taipei City 106, Taiwan
T. +886 2 6631 1000 F. +886 2 6631 1001 E. stli@iii.org.tw

財團法人資訊工業策進會 科技法律研究所
INSTITUTE FOR INFORMATION INDUSTRY
SCIENCE & TECHNOLOGY LAW INSTITUTE

TPIPAS官網

TPIPAS FB粉絲團