SafeLink 博創資訊科技股份有限公司
SafeLink Information Technology Co., Ltd.

TPIPAS

台灣個人資料保護與管理制度規範

版次：2012 V.1

公告施行日期：2012 年 09 月 04 日

資料來源 (TPIPAS官網)：http://www.tpipas.org.tw/model.aspx?no=159

中 華 民 國 102 年 07 月 01 日

0.前言

0.1 概述

臺灣個人資料保護與管理制度規範(Taiwan Personal Information Protection and Administration System, TPIPAS)(以下稱「本制度規範」)是使事業以「PDCA 方法論」，建立一套將個人資料保護與事業營運連結之系統化管理制度。

0.2 訂定目的

本制度規範旨在提升事業對於個人資料之保護與管理能力，降低營運風險，並創造可信賴之個人資料保護及隱私環境。

0.3 用途

本制度規範係對於事業之個人資料管理制度進行內、外部評量及用以核發事業「資料隱私保護標章」(Data Privacy Protection Mark, DP Mark)之依據。

0.4 PDCA 方法論

本制度規範之架構以「計畫-執行-檢查-行動(Plan-Do-Check-Act)，PDCA 方法論」為基礎。說明如下：

(1) 計畫：建立個人資料保護管理政策、目標及相關程序。

(2) 執行：個人資料管理制度之實施。

(3) 檢查：依據個人資料保護管理之政策、目標及要求，評估與監督流程及其產出，並將結果回報給最高管理階層加以審查。

(4) 行動：採取措施，以持續改善個人資料管理制度之績效。

1.適用範圍

本制度規範係針對蒐集、處理、利用及國際傳輸個人資料之事業，訂定相關規範事項，以建立個人資料管理制度，確保個人資料之安全。

2.版本標示

事業引用本制度規範，應註明所引用版本。若未註明者，則指使用最新版本。

3.用語與定義

本制度規範用詞，定義如下：

3.1 個人資料管理制度

指事業針對所持有個人資料所訂定之政策、內部管理組織及其規則、風險管控措施、應變處理程序及教育訓練計畫之整體管理體系。

3.2 個人資料

指包含自然人姓名、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。

3.3 當事人

指透過個人資料得以識別之本人。

3.4 事業

指法人或非法人團體。

3.5 個人資料管理代表

指最高管理階層指派管理階層之一，就事業內部個人資料管理制度之運作具有監督管理權責之人。

3.6 個資管理人員

實際推動並確保個人資料管理制度之有效運作之人員。

3.7 事業人員

指受事業直接監督，包括正職、派遣及其他與事業保有個人資料之蒐集、處理或利用有關之從業人員。

3.8 事故

指事業之個人資料外洩、滅失、毀損、竄改及其他侵害；或其他違反個人資料保護相關法令或本制度規範之情事。

4.要求事項

4.1 一般要求事項

事業應依其規模、特性及本制度規範之具體要求，建立、實施與維持其個人資料管理制度，並持續改善，以維護其有效性。

4.2 個人資料保護管理政策

事業應將其內部保有及管理個人資料之依據、目的與事業所負責任等基本理念原則，以書面訂定並對事業人員加以公開周知。

4.3 個人資料保護管理手冊

事業為建置個人資料管理制度，應製作個人資料保護管理手冊，訂定具體規則，並提出有效方式維持機制運作，供事業依循使用。

具體規則內容至少包括：

(1) 識別法令與其他相關規範。

(2) 識別事業所保有之個人資料。

(3) 事業蒐集、處理或利用個人資料之事宜。

(4) 個人資料相關之風險分析及管控措施。

(5) 事故緊急應變。

(6) 事業各部門以及層級所擁有個人資料管理權限與責任。

(7) 當事人權利之行使。

(8) 維持個人資料正確性。

(9) 安全管理措施。

(10) 事業人員之監督與獎懲。

(11) 委託蒐集、處理或利用個人資料之監督。

(12) 教育訓練。

(13) 個人資料管理制度之文件與紀錄管理。

(14)當事人申訴及諮詢。

(15)內部評量。

(16)矯正及預防措施。

(17)最高管理階層定期檢視。

4.4 個別要求事項

4.4.1 識別法令及其他相關規範

事業應識別所須遵循之相關法令，明示其個人資料管理制度與國家個人資料保護相關法規在內容及執行面上之相符性，並依法令之變動進行調整。

4.4.2 納入管理之個人資料範圍

事業應識別其保有之個人資料檔案，及蒐集、處理、利用個人資料之流程，劃定其納入個人資料管理制度之範圍，建立並維護個人資料檔案清冊及流程說明。

4.4.3 風險管控措施

事業應就納入管理範圍之個人資料，識別事業因蒐集、處理、利用個人資料可能面臨的風險，視需求訂定管控措施。

4.4.4 資源管理

事業應提供並維持個人資料管理制度所需之人力及軟硬體資源，確保相關資源管理之實施、維持及改善方式之有效性，並就資源管理事項留存相關紀錄。

4.4.5 權限與責任分工

事業應以書面明定個人資料管理制度之相關人員之職務、職掌、選任方式、責任層級及權限內容，並向事業內部公開周知。

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，事業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) 防止事業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。

4.5 管理制度之實施

4.5.1 基本原則

事業應確保個人資料之蒐集、處理、利用或國際傳輸，以誠實信用方式進行，出於最小且未逾越特定目的之必要範圍，並與蒐集之目的具有正當合理之關聯。

4.5.1.1 蒐集

事業針對個人資料之蒐集程序應符合下列要求：

(1) 確認蒐集時具備特定目的，並符合法律規定之特定情形。

(2) 其他法令規定蒐集時應履行之義務。

(3) 保存前二款相關紀錄。

4.5.1.2 處理

事業為建立或利用個人資料檔案，針對個人資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結及進行內部傳送，其程序應符合下列要求：

(1) 確認處理時符合蒐集時之特定目的及特定情形。

(2) 其他法令規定處理時應履行之義務。

(3) 事業應訂定適當且合法程序，處理刪除暨銷毀及業務終止時事業所保有之個人資料。

(4) 保存前四款相關紀錄。

4.5.1.3 利用

事業對於個人資料之利用程序應符合下列要求：

(1) 於蒐集之特定目的必要範圍之內利用個人資料。

(2) 目的外利用個人資料時係屬合乎法律要求。

(3) 保存前二款相關紀錄。

4.5.1.4 行銷

事業針對利用個人資料進行行銷，其程序應符合下列要求：

(1) 提供當事人至少首次免費表示拒絕接受行銷之方式。

(2) 當事人可隨時拒絕接受行銷之管道，並於表示拒絕接受後，立即停止利用其個人資料為行銷之用途。

(3) 保存前二款相關紀錄。

4.5.1.5 特種個人資料之蒐集、處理及利用限制

事業針對醫療、基因、性生活、健康檢查、犯罪前科等特種個人資料，其程序應符合下列要求：

(1) 內部人員原則禁止蒐集、處理及利用特種個人資料之要求。

(2) 例外得蒐集、處理或利用特種個人資料時，係屬合乎法律要求。

(3) 保存前二款相關紀錄。

4.5.1.6 告知義務之履行

事業針對個人資料保護法規定之應告知事項，應建立告知程序暨免告知之確認程序，其內容至少符合下列要求：

(1) 符合個人資料保護相關法律之告知時點。

(2) 適當之告知方式。

(3) 針對免告知之理由及其確認方式。

(4) 保存前三款相關紀錄。

4.5.2 當事人之相關權利

4.5.2.1 個人資料之相關權利

事業應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。

4.5.2.2 當事人行使權利之程序事項

事業為處理 4.5.2.1 之當事人請求之程序，內容至少符合下列要求：

(1) 具備當事人提出請求之方式。

(2) 具備確認當事人身分之方式。

(3) 具備確認事業是否得依法拒絕當事人行使其權利。

(4) 具備拒絕請求或發生爭議，當事人得提出申訴之管道與聯繫方式。

4.5.2.3 提供查詢、閱覽、複製本之方式

事業針對當事人請求查詢、閱覽個人資料或製給個人資料複製本，其程序應符合下列要求：

(1) 確保於 15 日內為准駁之決定。

(2) 准駁當事人請求，拒絕時並應附理由以書面通知當事人。

(3) 決定延長 15 日作出准駁之決定時，應附理由以書面通知當事人。

(4) 保存前三款相關紀錄。

4.5.2.4 當事人請求個人資料補充、更正、刪除、停止蒐集、處理及利用程序

事業針對當事人請求補充、更正、刪除、停止蒐集、處理或利用個人資料，其程序應符合下列要求：

(1) 確保於 30 日內為准駁之決定。

(2) 准駁當事人請求，拒絕時並應附理由以書面通知當事人。

(3) 決定延長 30 日作出准駁之決定時，應附理由以書面通知當事人。

(4) 保存前三款相關紀錄。

4.5.2.5 申訴及諮詢之處理

針對申訴與諮詢事項，事業應確保迅速有效之處理，其程序應符合下列要求：

(1) 適當且迅速回應當事人。

(2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。

(3) 保存前二款相關紀錄。

4.5.3 管理監督

4.5.3.1 維持個人資料之正確性

事業為維持個人資料正確之狀態，應建立符合下列要求之程序：

(1) 確保個人資料於處理過程中，正確性不受影響。

(2) 當確認個人資料有錯誤時，應適時更正。

(3) 檢查個人資料之正確性。

(4) 因可歸責於事業之事由，未為更正或補充之個人資料，應訂定於更正或補充後，通知曾提供利用對象。

4.5.3.2 安全管理措施

事業應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。

必要且適當之安全管理措施應至少包括：

(1) 作業面安全管理措施

(2) 物理性安全管理措施

(3) 技術性安全管理措施

4.5.3.3 事業人員之監督

事業應對事業人員就個人資料蒐集、處理及利用採取必要且適當之監督措施。

4.5.3.4 委託蒐集、處理或利用個人資料之監督

事業委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項：

(1) 委託人及受託人之權利義務。

(2) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。

(3) 受託人對個人資料之安全管理措施。

(4) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意。

(5) 向委託人報告關於個人資料處理狀況之內容以及報告週期。

(6) 委託人對受託人保留指示之事項。

(7) 發生事故時向委託人即時報告及採行之補救措施等相關事項。

(8) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。

(9) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反本法或基於本法所發布之命令規定之情事，應立即通知委託人。

委託人應定期確認受託人執行之狀況，並將確認結果紀錄之。

4.6 教育訓練

4.6.1 一般要求

事業應以適當方式確保事業人員對個人資料管理具有正確的認知及能力。

4.6.2 基本教育訓練

事業針對事業人員應提供必要的個人資料管理教育訓練。

4.6.3 權責人員教育訓練

事業應決定個人資料管理制度相關權責人員之必要能力與教育訓練需求，並規劃與執行。

4.6.4 成果維持及改善措施

事業應針對事業人員教育訓練成果建立紀錄與改善機制。

📖 5.管理責任

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

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。

5.3 個資管理人員

事業應由取得下列資格之一者，擔任個資管理人員，以實際推動並確保個人資料管理制度之有效運作：

(1) 個人資料管理師。

(2) 個人資料內評師。

(3) 個人資料驗證師。

個資管理人員得由個資管理代表兼任。

📖 6.有效性量測

事業應針對個人資料管理制度之實施，建立分析量測機制，藉由使用各項方式，使管理代表能判定個人資料管理制度內所建立之程序與機制是否有效，將所進行之分析量測作成紀錄，以確保制度之持續有效運作。

📖 7.文件及紀錄之控管

📃 7.1 文件及紀錄之範圍

7.1.1 文件

事業應製作及保存下列文件：

(1) 個人資料保護管理政策。

(2) 個人資料保護管理手冊，及其相關具體規則。

(3) 個人資料內部管理程序相關表單。

7.1.2 紀錄

事業應製作及保存實施個人資料管理制度之相關紀錄。

📃 7.2 文件管理

事業為落實個人資料管理制度，應建立文件管理程序，其程序包含：

(1) 文件之製作及修正之相關事項。

(2) 明確標記文件修正時，與前次版本間之關聯及差異。

(3) 文件之儲存位置與保存方式及其存取權限。

📃 7.3 記錄管理

事業為落實且證明其已符合本制度所要求之事項，應製作必要之紀錄文件並確立實施相關之管理程序。

📖 8.內部評量

事業每年應依其特性規劃執行內部評量，以瞭解個人資料管理制度是否符合下列要求：

(1) 符合法規及本制度之要求。

(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。

事業應規劃內部評量方式及流程，以決定內部評量之準則、範圍、頻率及方法。

事業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。

內部評量應由具備個人資料內評師或個人資料驗證師資格者執行，並由其出具內部評量報告。

📖 9.改善

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。

最高管理階層決策調整個人資料管理制度時，應考量以下事項，並據以調整與修正個人資料管理制度：

(1) 檢視報告。

(2) 社會情勢、國民認知、技術發展等各種環境之變遷。

(3) 事業業務領域之變化。

(4) 事業內外部之改善建議。

(5) 其他可能影響個人資料管理制度的任何變更。

9.2 矯正及預防措施

事業針對內部評量及本管理制度實施之結果，應規劃矯正措施及預防措施，並確保相關措施之執行。

9.2.1 矯正措施

事業針對不符合事項，應規劃及完成執行矯正措施，並完成以下事項：

(1) 確認不符合事項之內容並判定其發生原因。

(2) 評估需求並提出矯正方案，以確保不符合事項不再發生。

(3) 訂定合理之執行期限。

(4) 紀錄執行結果。

(5) 檢視所採取的矯正方案成果。

9.2.2 預防措施

事業針對潛在不符合事項之風險，應規劃及執行預防措施時，並完成以下事項：

(1) 依據事業因持有個人資料可能面臨的風險，確認各項潛在不符合事項之內容及其原因。

(2) 評估需求並提出預防方案，以確保不符合事項發生。

(3) 訂定合理之執行期限。

(4) 紀錄執行結果。

(5) 檢視所採取的預防方案成果。