

臺灣個人資料保護與管理制度規範

TPIPAS : 2021⁺

TPIPAS 維運機構

財團法人資訊工業策進會

科技法律研究所

臺灣個人資料保護與管理制度規範

TPIPAS：2021⁺

修正與公告日期：2026 年 06 月 01 日

0. 簡介

0.1. 概述

臺灣個人資料保護與管理制度規範（以下稱「本制度規範」）是使組織以「PDCA 方法論」，建立一套將個人資料保護與組織營運連結、符合我國個人資料保護相關法令與國際隱私保護趨勢之系統化管理制度。

0.2. 訂定目的

本制度規範旨在提升組織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

本制度規範係對於組織之個人資料管理制度進行內、外部評量及用以核發組織「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、利用或國際傳輸個人資料之組織，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

組織引用本制度規範，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

指組織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. 組織

指公務機關或自然人以外之非公務機關。

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，就組織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. 個人資料管理人員

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. 查核人員

指為辦理組織個人資料安全稽核，具有稽核之獨立性及專業性之人員。組織應要求查核人員與執行個人資料管理之管理人員不得互相兼任。

3.8. 組織人員

指受組織直接監督，包括正職、派遣及其他與組織保有個人資料之蒐集、處理或利用有關之從業人員。

3.9. 事故

指組織之個人資料外洩、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. 組織環境

4.1. 內外部議題

組織應決定與個人資料管理制度有關且可能影響制度運行有效性之內部與外部議題。

4.2. 利害關係人需求

組織應決定與個人資料管理制度相關之利害關係人，以及與利害關係人有關之要求事項。

4.3. 管理制度範圍

組織應考慮 4.1 及 4.2 事項決定個人資料管理制度之範圍。

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) 決定個人資料管理制度目標，確保符合組織需求與發展策略。
- (2) 決定個人資料保護管理政策。
- (3) 決定資源管理。
- (4) 決定個人資料保護管理組織架構及權責劃分。
- (5) 定期檢視管理制度，確保管理制度達成預期效果。
- (6) 建立有效之溝通機制，適時指導與支援組織人員。
- (7) 傳達落實個人資料管理制度之重要性。

5.2. 個人資料保護管理政策

最高管理階層應將其內部保有及管理個人資料之依據、目的與組織所負責任等基本理念原則，以書面訂定並對組織人員加以公開周知。個人資料保護管理政策應包括以下事項：

- (1) 個人資料管理制度之目標。
- (2) 承諾落實本制度規範要求事項與法令。
- (3) 承諾定期檢視與持續改善。

5.3. 權限與責任分工

最高管理階層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，並向組織內部公開周知。

5.4. 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之各項程序被建立、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。

5.5. 個人資料管理人員

組織應由取得下列資格之一者，擔任個人資料管理人員，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。

個人資料管理人員得由個人資料管理代表兼任。

6. 制度規劃

6.1. 總則

組織應依其規模、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。

6.2. 個人資料保護管理手冊

組織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，供組織依循使用。

具體規則內容至少包括：

- (1) 識別法令與其他相關規範。
- (2) 識別組織所保有之個人資料。
- (3) 組織蒐集、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) 組織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) 組織人員之監督與獎懲。
- (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。
- (18) 個人資料或資通安全維護計畫。

6.3. 因應風險之規劃

組織於規劃個人資料管理制度時應將內外部議題、利害關係人需求與相關本制度規範納入考量，規劃風險管理之原則、框架及過程，辨識相關風險與因應管控措施，並得適時採納從設計與預設階段著手隱私保護 (Privacy by design and default) 之概念。

6.3.1. 個人資料隱私衝擊風險評鑑

組織應建立與維持個人資料相關之風險分析與評估程序，風險分析與評估程序應包括以下事項：

- (1) 建立與維護個人資料風險準則，包括風險接受準則與實施個人資料風險分析與評估之準則。

- (2) 確保重複之個人資料風險分析與評估產生一致、有效及可比較之結果。
- (3) 識別個人資料風險與風險擁有者。
- (4) 分析個人資料風險，包括風險實現時可能導致之潛在後果、風險發生之實際可能性與決定風險等級。
- (5) 評估個人資料風險，包括比較風險分析結果與訂定已分析風險之風險處理優先次序。
- (6) 所識別風險應包括組織與當事人之影響。

6.3.2. 風險管控措施

組織應考量個人資料隱私衝擊風險評鑑結果，決定適當之個人資料風險管控措施，並確保符合附表 A 所列必要管理措施。

7. 支援

7.1. 資源

組織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。

7.2. 教育訓練

7.2.1. 總則

組織應以適當方式確保組織人員對個人資料管理、管理與獎懲制度具有正確之認知及能力。

7.2.2. 基本教育訓練

組織針對組織人員應定期提供必要之個人資料管理教育訓練。

7.2.3. 權責人員教育訓練

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

7.2.4. 成果維持及改善措施

組織應針對組織人員定期教育訓練成果建立紀錄與持續改善機制。

7.3. 文件及紀錄之控管

7.3.1. 文件及紀錄之範圍

7.3.1.1. 文件

組織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。

7.3.1.2. 紀錄

組織應製作及保存實施個人資料管理制度之相關紀錄。

7.3.2. 文件管理

組織為落實個人資料管理制度，應建立文件管理程序，其程序包括：

- (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。

7.3.3. 使用紀錄與證據管理

組織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，其紀錄包括：

- (1) 個人資料之蒐集、處理或利用紀錄。
- (2) 落實安全維護措施之證據。
- (3) 當事人權利行使之紀錄。
- (4) 保存前三款相關紀錄，應留存至少五年。

7.3.4. 系統日誌管理

組織維運其資通系統蒐集、處理或利用個人資料，應執行下列事項：

- (1) 訂定日誌之記錄時間週期及留存政策，並保存適當時間。
- (2) 確保資通系統具備記錄特定事件之功能，並決定應記錄之特定資通系統事件。
- (3) 記錄資通系統管理者帳號所執行之各項功能。

7.4. 溝通或傳達

組織應建立有效之溝通或傳達機制與程序。

8. 個人資料管理制度之實施

8.1. 識別法令及其相關規範

組織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。

8.2. 納入管理之個人資料範圍

組織應界定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。

8.3. 風險管控措施之實施

組織應就納入管理範圍之個人資料，識別組織因蒐集、處理、利用個人資料可能面臨之風險，考量個人資料隱私衝擊風險評鑑結果，落實適當風險管控措施。

8.4. 個人資料之蒐集、處理與利用

8.4.1. 總則

組織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。

8.4.2. 蒐集

組織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。

8.4.3. 處理

組織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) 組織應訂定適當且合法之程序，處理刪除暨銷毀及業務終止時組織所保有之個人資料，並留存相關作業之方法、時間、地點及證明。
- (4) 保存前三款相關紀錄。

8.4.4. 利用

組織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) 其他法令規定利用時應履行之義務。
- (3) 保存前二款相關紀錄。

8.4.5. 行銷

組織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。

8.4.6. 國際傳輸

組織於國際傳輸個人資料時，應確實檢視並遵循主管機關對國際傳輸之限制；於傳輸前明確告知當事人擬傳輸之國家或區域，並保存相關紀錄。

8.4.7. 特種個人資料之蒐集、處理及利用限制

組織針對病歷、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) 組織人員原則禁止蒐集、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，符合法律規定之特定情形。
- (3) 針對載有特種個人資料之紙本或電子檔案，應採取適當之資料安全管理措施。
- (4) 保存前三款相關紀錄。

8.4.8. 告知義務之履行

組織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。

8.5. 當事人之相關權利

8.5.1. 個人資料之相關權利

組織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。

8.5.2. 當事人行使權利之程序事項

組織為處理前條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) 具備確認組織是否得依法拒絕當事人行使其權利之方式。
- (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。
- (5) 確保當事人行使權利於法令規定期間內為准駁之決定。
- (6) 准駁當事人請求，拒絕時並應附理由以書面通知當事人。
- (7) 決定延長於法令規定期間作出准駁之決定時，應附理由以書面通知當事人。
- (8) 保存相關紀錄。

8.5.3. 申訴及諮詢之處理

針對申訴與諮詢事項，組織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，必要時應通報個人資料管理代表，並由其決定回應之內容與方式。
- (3) 保存前二款相關紀錄。

8.6. 維持個人資料之正確性

組織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) 因可歸責於組織之事由，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。

8.7. 安全管理措施

組織應針對因蒐集、處理及利用個人資料所可能面臨之風險，採取防止個人資料被竊取、竄改、毀損、滅失或洩漏之必要且適當之安全管理措施。

如附表 A 所示，必要且適當之安全管理措施應至少包括，但不限於下列措施：

- (1) 管理面安全管理措施。
- (2) 技術面安全管理措施。

8.8. 組織人員之監督

組織應對組織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。

8.9. 委託蒐集、處理或利用個人資料之監督

組織委託他人蒐集、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) 選任受託人辦理受託業務之相關程序及環境，應具備完善之安全管理措施或通過公正第三方驗證。
- (3) 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。
- (4) 受託人對個人資料之安全管理措施。
- (5) 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，應得委託人同意且應具備完善之安全管理措施。
- (6) 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。
- (7) 委託人對受託人保留指示之事項。
- (8) 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。
- (9) 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。
- (10) 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法律或基於法律所發布之命令規定之情事，應立即通知委託人。

組織應定期確認與審查受託人執行之狀況，並將確認結果記錄之。

8.10. 事故之緊急應變

為避免事故可能產生之不利益及影響，組織應訂定並落實事故緊急應變措施。相關措施應至少包括：

- (1) 知悉事故時於適當時機及方式通知當事人事故發生，並提供後續查詢與處理管道。
- (2) 採取即時有效之應變措施，防止事故之擴大，及記載相關事實、影響、已採取之因應措施，並保存相關紀錄。

- (3) 避免類似事件再次發生之方法。
- (4) 將事故即時通報主管機關及其他依組織所識別之法令應通報之政府機關。
- (5) 將事故即時通報授證機關。

組織應將通知或通報之內容、方式、時限與通報範圍、應變措施及紀錄保存，以供備查。

9. 績效評估

9.1. 有效性量測

組織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與改善。

9.2. 內部評量

組織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。

組織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。組織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。

內部評量計畫應由具備個人資料內評師或個人資料驗證師資格者規劃，並由其確保內部評量執行之有效性與出具內部評量報告。

9.3. 定期檢視

個人資料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) 個人資料保護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) 組織業務領域之變化。

- (4) 組織內外部之改善建議。
- (5) 其他可能影響個人資料管理制度之任何變更。

10. 改善

10.1. 總則

組織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。

10.2. 矯正措施

組織針對不符合事項，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) 記錄執行結果。
- (5) 檢視所採取之矯正方案成果。

10.3. 預防措施

組織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) 依據組織因持有個人資料可能面臨之風險，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，以確保不符合事項不再發生。
- (3) 訂定合理之執行期限。
- (4) 記錄執行結果。
- (5) 檢視所採取之預防方案成果。
- (6) 持續改善個人資料管理制度。

11. 個人資料管理制度實施指引

11.1. 總則

組織宜考量其規模、特性與需求，針對本管理制度實施指引建立並落實相關程序。

11.2. 從設計與預設階段著手隱私保護

組織宜於產品、服務或系統等開發設計階段時，落實本制度規範、個人資料保護法與相關法令之精神。

11.3. 生物特徵個人資料

組織於蒐集、處理或利用指紋、掌紋或臉部辨識等生物特徵個人資料，宜遵循個人資料保護法關於特種個人資料等相關法令。

11.4. 風險處置

組織針對於個人資料隱私衝擊風險評鑑結果為高風險之行為或流程，且風險無法透過風險管控措施緩解時，宜事先與相關主管機關溝通或諮詢。

11.5. 當事人同意

組織於取得當事人同意時，宜注意當事人同意給予之真摯性、自主性、任意性、具體特定且受充分告知。

組織於當事人撤回同意時，其當事人撤回同意之方式宜與給予同意之方式等同便利。

11.6. 當事人權利

組織宜建立並落實相關程序，以回應當事人行使下列權利：

- (1) 修改或撤回同意權
- (2) 反對權
- (3) 限制處理權
- (4) 資料近用權
- (5) 資料可攜權
- (6) 資料更正權
- (7) 資料刪除權

11.7. 未成人之保護

組織於蒐集、處理或利用未成人個人資料時，宜有較高之注意義務與安全管理措施，並應確認已採取措施足辨識未成年之法定代理人已有效代為同意，或足辨識具其他符合法律規定之特定情形。

11.8. 無障礙

組織於運行個人資料管理制度時，宜考量身心障礙者權益，並以適當方式協助之。

11.9. Cookie

組織於蒐集、處理或利用 Cookie 等類似科技，宜僅於必要範圍內為之，並取得當事人之同意與提供當事人拒絕之選項。

11.10. 暫存檔之處理

組織於蒐集、處理或利用個人資料所產生之暫存檔，宜確保於適當時間內刪除或銷毀。

11.11. 自動化決策與剖繪

組織於使用自動化決策、剖繪等類似科技且影響當事人權益時，宜賦予當事人請求人為介入之機會。

11.12. 國際傳輸

組織如有個人資料國際傳輸之流程，宜取得亞太經濟合作（Asia-Pacific Economic Cooperation, APEC）之跨境隱私規則（Cross-Border Privacy Rules, CBPR）驗證或全球跨境隱私規則（Global CBPR）驗證歐盟一般資料保護規則（General Data Protection Regulation, GDPR）所定認證或驗證。

11.13. 委託蒐集、處理或利用個人資料之監督

組織於委託他人蒐集、處理或利用個人資料之全部或一部時，宜確保受託人落實附表 A 所列安全管理措施。

11.14. 應對政府存取資料

組織應建立應對程序，回應要求揭露組織所持有之個人資料之國內、外司法或其他政府傳票、搜索令或其他命令，其內容應包括：

- (1) 確認要求與回應方式符合法律規定之特定情形。
- (2) 保存相關紀錄。

附表 A：本制度規範安全管理措施

修正與公告日期：2026 年 06 月 01 日

附表 A 係針對本制度規範管理措施制定基本安全管理具體措施，組織應制定符合附表 A 所列各項管理措施，確保組織蒐集、處理及利用個人資料流程符合法令遵循，並已採取防止個人資料被竊取、竄改、毀損、滅失或洩漏之必要且適當之安全管理措施。

A8.7 資通安全

A8.7.1 存取控制

管理目標：組織對個人資料之存取加以規範與保護，防止任何未經授權之存取與破壞。

管理措施：

1. 存取控制政策

組織應透過存取控制政策與存取實施機制（如存取控制清單）對個人資料之存取進行管控。

2. 帳號管理

組織應建立帳號管理機制，包括帳號之申請、開通、停用、去識別化或刪除之程序，並應至少每年定期辦理帳號清查，或就特權帳號評估設定較高頻率之清查週期，以檢視並刪除或禁用已逾期之臨時或緊急帳號、閒置帳號，及其他不再使用或有異常情形之帳號。當使用者逾組織所訂定之閒置時間未進行操作時，系統應自動將其登出。

3. 職責分工

組織對於個人資料之存取應落實職責分工。

4. 最小權限

組織應識別業務內容涉及個人資料蒐集、處理或利用之人員，並落實最小權限之概念，僅允許使用者依組織任務與業務功能需要，完成指派任務授權之存取行為。

5. 遠端存取

組織應透過政策訂定選擇禁止或嚴格限制遠端存取個人資料，倘允許遠端存取，組織應確保傳輸過程經過適當加密，並應建立自動監控措施，以確保從遠端連線至資通系統之活動，均符合遠端存取政策。

6. 行動裝置存取

組織應透過政策訂定選擇禁止或嚴格限制，來自於可攜式或行動裝置對個人資料之存取。如果行動裝置經允許存取個人資料，組織應確保該裝置被適當保護，並定期檢視或確認該裝置

	<p>以確認其安全狀態。</p> <p>7. 資訊分享</p> <p>組織應制定個人資料資訊分享機制，該機制應保存分享方式與對象之紀錄，並確保對個人資料存取之授權符合政策規定。</p>
<p>A8.7.2 事件日誌與可歸責性</p>	<p>管理目標：組織依據個人資料風險評鑑與業務所需，決定資訊系統需要被稽核與記錄之事件，並建立監控機制。</p> <p>管理措施：</p> <ol style="list-style-type: none"> 1. 記錄事件 <p>組織應監控影響個人資料機密性、完整性之事件，例如對個人資料之未授權存取或修改。</p> 2. 日誌紀錄之檢視、分析、通報 <p>組織應定期檢視與分析資通系統之日誌紀錄，以發現可能影響個人資料機密性或完整性之不當或異常活動跡象；並應就可疑活動或疑似違規情形進行調查，將調查結果報告權責主管，並採取適當措施。</p> 3. 日誌紀錄之保存與維護 <p>組織應訂定日誌之紀錄時間周期及留存政策，並採取措施避免紀錄遭毀損或竄改。如對日誌之存取管理，僅限於有權限之使用者。</p>
<p>A8.7.3 識別鑑別</p>	<p>管理目標：組織對於組織內部之系統使用者，應有特定之方式確認其所擁有之存取帳號與權限，以確保行為之明確可歸責性。</p> <p>管理措施：</p> <ol style="list-style-type: none"> 1. 使用者之識別與鑑別 <p>組織內之使用者使用資通系統，組織應賦予其唯一之識別與驗證方式，避免使用共用帳號。</p> 2. 身分驗證管理 <p>使用預設密碼登入系統時，應於登入後要求立即變更。身分驗證相關資訊應採安全傳輸機制不以明文方式傳送。應依需要制定並落實密碼規則與更新週期，落實密碼管理原則。</p>

<p>A8.7.4 媒體安全</p>	<p>管理目標：組織應確保儲存個人資料之媒體，其存取、保存、傳輸與汰除時之安全。</p> <p>管理措施：</p> <ol style="list-style-type: none"> 1. 媒體存取 組織應採用特定防護措施，對特定授權人員，限制其對數位與非數位媒體類型之存取。 2. 媒體儲存 組織應建立並落實個人資料媒體儲存之安全作業規定。 3. 媒體傳輸 個人資料儲存媒體運輸或傳輸到管控區域外時，應採用適當安全防護措施。 4. 媒體汰除 組織於媒體汰除時應透過適當程序加以安全汰除，確保無法被還原。
<p>A8.7.5 實體與環境安全</p>	<p>管理目標：防止儲存個人資料場所受人為因素未授權入侵與存取而導致個人資料之洩漏或毀損。</p> <p>管理措施：</p> <ol style="list-style-type: none"> 1. 實體存取控制 組織應識別儲存個人資料之安全周界，於存放個人資料場所，如資訊機房及檔案庫房，採取適當安全措施，並針對進入場所之權限加以管控。 2. 實體存取監視 組織應定期檢視已實施安全措施之有效性，並就人員及個人資料之進出，建立監視與環境控管安全機制，並制定合理保存期間，保存相關出入紀錄。
<p>A8.7.6 資訊傳輸</p>	<p>管理目標：防止個人資料傳輸時遭未授權揭露。</p> <p>管理措施：</p> <ol style="list-style-type: none"> 1. 邊界保護 組織於系統外部邊界與系統內部之關鍵內部邊界，應建立適當監視與控制通訊之介面防護。 2. 傳輸機密性

	<p>組織應採取適當措施確保個人資料傳輸之機密性，並提供傳輸加密協定之設定截圖、加密證明文件或傳輸軌跡紀錄。</p>
<p>A8.7.7 系統與資訊完整性</p>	<p>管理目標：確保個人資料資通系統安全控管措施之有效性。</p> <p>管理措施：</p> <ol style="list-style-type: none"> 1. 安全性檢測 <p>組織應進行資通系統脆弱性識別、報告與修正作業。系統更新前應事先進行測試，瞭解該更新對資通系統可能產生之結果與衝擊。</p> 2. 惡意程式防護 <p>組織應針對資通系統可能之出入端點部署有效之惡意程式防護機制。防毒軟體應設定自動更新至最新版本之病毒碼，並啟用即時防護功能；另應定期執行完整系統掃描，並依程序針對偵測到之惡意程式進行隔離、刪除或其他適當處置。</p> 3. 資通系統監看 <p>組織應透過資通系統監視內向與外向通訊，發現資通系統有被入侵跡象時，依程序通報特定人員。</p> 4. 測試環境管理 <p>組織應區隔正式環境與測試環境，且應避免使用真實個人資料作為系統之測試資料。如有使用真實個人資料測試系統之必要，應制定程序及安全使用規範，依循程序申請使用。</p>
<p>A8.7.8 系統發展生命週期階段之安全性</p>	<p>管理目標：確保組織系統發展之安全需求（含機密性、完整性、可用性、遵循性）。</p> <p>管理措施：</p> <ol style="list-style-type: none"> 1. 組織應運用安全系統發展生命週期（SSDLC）概念於系統發展生命週期之需求評估、設計開發、測試及部署與維運階段，合理滿足系統之安全需求。 2. 資通系統如涉及個人資料之蒐集、處理或利用，

	<p>應於系統發展及維運各階段，依相關法規導入適當之安全措施，包括帳號管理與身分鑑別、存取控制、隱碼及加密、日誌紀錄與監控、入侵防護及備份等機制。</p> <ol style="list-style-type: none"> 3. 組織資通系統開發、維運如委外辦理，應將系統發展生命週期各階段所必要之安全需求納入委外契約。 4. 提供對外服務之資通系統，於上線前應辦理源碼檢測、弱點掃描及滲透測試，並完成弱點、漏洞修補作業；系統上線後應持續辦理。 5. 組織應定期評估各項安全措施之有效性，並持續檢討及改善。
A8.7.9 網路安全防護	<p>管理目標：確保組織網路系統有效應對威脅與風險。</p> <p>管理措施：組織應制定有效網路安全防護政策，如定期維護網路設備軟硬體、韌體及元件，避免系統遭未授權存取、入侵，損害資料之機密性、完整性與可用性，並保存相關更新之紀錄。</p>
A8.7.10 新興技術風險管理	<p>管理目標：確保組織於採納及運用新興技術時，能適當識別、評估並管理其所衍生之相關風險。</p> <p>管理措施：組織應制定新興技術相關政策，就新興技術之採納與運用進行適當之風險評估及管理。</p> <ol style="list-style-type: none"> 1. 資通系統如部分或全部採用雲端服務，應就其取得、環境設定及維運管理訂定相關規範，並確保儲存於雲端之個人資料安全（如存取控制、資料加密、備份機制之建立），並定期檢視與更新。 2. 組織如開發、部署或採購人工智慧系統或服務，應就其取得、環境設定及使用管理訂定相關規範。

A8.7.11 資料可用性維護	<p>管理目標：確保組織所留存之個人資料具實現蒐集目的所必要之可用性，減少因個人資料減失或無法存取致當事人受侵害之風險。</p> <p>管理措施：組織應訂定資料備份之政策，決定資料備份之合理頻率，並定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。備份資料應採與原始資料相同之安全防護措施，確保其機密性與完整性不受影響。</p>
A8.8 組織人員之管理與監督	
A8.8.1 選任監督	<p>管理目標：確保組織人員適任其角色。</p> <p>管理措施：組織聘用人員時，應進行適當篩選。</p>
A8.8.2 保密契約	<p>管理目標：確保組織人員瞭解其所承擔之責任。</p> <p>管理措施：組織與人員簽訂僱傭或委任契約時，應一併簽訂個人資料相關保密契約，並確保於人員離職或職務變動時，異動人員有義務配合個人資料媒介物之交接、返還或資料刪除措施；同時，異動人員於合理期間內仍須負有保密義務。</p>
A8.8.3 教育訓練	<p>管理目標：確保組織人員獲得應有資通安全專業課程訓練或資通安全職能訓練，以利管理制度推動與運作。</p> <p>管理措施：組織應制定教育訓練計畫，並訂定評量機制。</p>