法規名稱：私立職業訓練機構個人資料檔案安全維護計畫及處理辦法

修正日期：民國 111 年 03 月 18 日

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

本辦法適用對象為職業訓練法第五條第二款及第三款所定之私立職業訓練機構。

第 3 條

1 私立職業訓練機構為落實個人資料檔案之安全維護及管理，以防止個人資料被竊取、竄改、毀損、滅失或洩漏，應訂定個人資料檔案安全維護計畫（以下簡稱本計畫）。

2 本計畫內容，應包含下列事項：

一、個人資料保護規劃。

二、個人資料管理程序。

三、其他個人資料檔案安全維護事項。

第 4 條

私立職業訓練機構對個人資料保護之規劃，應包括下列事項：

一、個人資料保護相關法令規定之遵守。

二、於特定目的範圍內，蒐集、處理及利用個人資料之合理安全方法。

三、於特定目的範圍外，利用個人資料之合理安全方法。

四、保護所蒐集、處理、利用之個人資料檔案之合理安全水準技術。

五、供當事人行使個人資料之相關權利、提出相關申訴及諮詢之聯絡窗口。

六、處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故之緊急應變程序。

七、委託蒐集、處理及利用個人資料者，監督受託者之機制。

八、確保個人資料檔案之安全，維持本計畫運作之機制。

第 5 條

1 私立職業訓練機構就個人資料檔案之安全維護管理，應指定適當人員或專責組織負責，並配置相當資源。

2 前項人員或專責組織之任務如下：

一、規劃、訂定、修正及執行本計畫。

二、定期對所屬人員施以基礎認知宣導或專業教育訓練，使其瞭解個人資料保護相關法令規定、責任範圍、管理措施或方法。

第 6 條

私立職業訓練機構應依據個人資料保護相關法令，清查所保有之個人資料，納入本計畫之範圍及建立檔案，並隨時確認有否變動。

第 7 條

私立職業訓練機構應依據前條所界定之範圍，分析蒐集、處理及利用過程中可能產生之風險，並依據分析結果，於本計畫中訂定適當管控措施。

第 8 條

1 私立職業訓練機構為因應所保有之個人資料被竊取、竄改、毀損、滅失或洩漏等事故，於本計畫中應建立下列機制：

一、應變處理機制：控制事故對當事人之損害。

二、事故調查機制：以適當方式通知當事人，並告知採取之因應措施。

三、檢討預防機制：避免類似事故再次發生。

2 私立職業訓練機構發生前項事故時，應於七十二小時內填具通報紀錄表（如附表），通報所在地之直轄市、縣（市）政府，並副知中央目的事業主管機關；中央目的事業主管機關或直轄市、縣（市）政府接獲通報後，得依本法第二十二條至第二十五條規定所賦予之職權，為適當之監督管理措施。

第 9 條

私立職業訓練機構就本法第六條第一項所定之個人資料，應於蒐集、處理或利用前，確認符合相關法令規定。

第 10 條

私立職業訓練機構為履行本法第八條及第九條所定之告知義務，於本計畫中應建立下列作業程序：

一、依據蒐集資料情況，採取適當之告知方式。

二、確認符合免告知當事人之事由。

第 11 條

私立職業訓練機構對個人資料之蒐集、處理或利用，除本法第六條第一項所定之資料外，於本計畫中應建立下列作業程序：

一、確認蒐集、處理個人資料符合特定目的及法定要件。

二、確認利用個人資料符合特定目的必要範圍；於特定目的外利用個人資料時，應檢視是否具備法定特定目的外之利用要件。

第 12 條

私立職業訓練機構利用個人資料行銷時，於本計畫中應建立下列作業程序：

一、利用個人資料行銷前，應讓當事人知悉並獲得同意。

二、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。

三、當事人表示拒絕接受行銷時，立即停止利用其個人資料行銷，並通知所屬人員。

第 13 條

1 私立職業訓練機構進行個人資料國際傳輸前，應檢視有無中央目的事業主管機關依本法第二十一條規定所為之限制，並告知當事人其個人資料所欲國際傳輸之區域。

2 前項個人資料國際傳輸，私立職業訓練機構應對資料接收方為下列事項之監督：

一、預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。

二、當事人行使本法第三條所定權利之相關事項。

第 14 條

當事人就其個人資料行使本法第三條所定之權利者，私立職業訓練機構於本計畫中應建立下列作業程序：

一、確認其為個人資料之本人或法定代理人。

二、提供當事人行使權利之方式，並依本法第十三條所定處理期限辦理。

三、確認有無本法第十條及第十一條得拒絕當事人行使權利之事由，拒絕時並附理由通知當事人。

四、查詢或請求閱覽個人資料或製給複製本者，告知得收取之費用標準或酌收必要成本費用。

第 15 條

私立職業訓練機構為維護其保有個人資料之正確性，於本計畫中應建立下列作業程序：

一、檢視個人資料於蒐集、處理或利用過程，有無錯誤。

二、定期檢查資料，發現錯誤者，適時更正或補充。未為更正或補充者，於更正或補充後，通知曾提供利用之對象。

三、有爭議者，依本法第十一條第二項規定就爭議資料之處理或利用，建立相關作業程序。

第 16 條

1 私立職業訓練機構應定期確認所保有個人資料之特定目的有無消失或期限屆滿。

2 個人資料之特定目的消失或期限屆滿時，應依本法第十一條第三項規定辦理。

第 17 條

私立職業訓練機構就人員管理，應採取下列措施：

一、確認蒐集、處理及利用個人資料之各相關業務流程之負責人員。

二、依據作業之需要，建立管理機制，設定所屬人員不同權限，並定期確認權限內容之適當及必要性。

三、與所屬人員約定保密義務。

四、所屬人員離職時取消其識別碼，並收繳其通行證（卡）及相關證件。

五、所屬人員持有個人資料者，於其離職時，應要求其返還個人資料之載體，並銷毀或刪除因執

行業務儲存而持有之個人資料。

第 18 條

私立職業訓練機構蒐集、處理或利用個人資料，就資料安全管理，應採取下列措施：

一、訂定作業注意事項。

二、運用電腦或自動化機器相關設備，訂定使用可攜式設備或儲存媒介物之規範。

三、保有之個人資料內容，有加密或遮蔽之必要時，採取適當之加密或遮蔽機制。

四、傳輸個人資料時，因應不同之傳輸方式，有加密必要時，採取適當加密機制，並確認資料收受者之正確性。

五、依據保有資料之重要性，評估有備份必要時，予以備份，並比照原件加密。儲存備份資料之媒介物，以適當方式保管，且定期進行備份資料之還原測試，以確保有效性。

六、儲存個人資料之媒介物於報廢或轉作其他用途時，以物理或其他方式確實破壞或刪除媒介物中所儲存之資料。

七、妥善保存管理機制及加密機制中所運用之密碼。

第 19 條

私立職業訓練機構就設備安全管理，應採取下列措施：

一、依據作業內容不同，實施必要之進出管制方式。

二、妥善保管個人資料之儲存媒介物。

三、針對不同作業環境，加強天然災害及其他意外災害之防護，並建置必要之防災設備。

第 20 條

私立職業訓練機構就技術管理，應採取下列措施：

一、於電腦、自動化處理設備或系統上設定認證機制，對有存取個人資料權限之人員進行識別及控管。

二、認證機制使用之帳號及密碼，具備一定之複雜度，並定期更換密碼。

三、於電腦、自動化處理設備或系統上設定警示與相關反應機制，以對不正常之存取進行適當之反應及處理。

四、個人資料存取權限之數量及範圍，依作業必要予以設定，且不得共用存取權限。

五、採用防火牆或入侵偵測等設備，避免儲存個人資料之系統遭受無權限之存取。

六、使用能存取個人資料之應用程式時，確認使用者具備使用權限。

七、定期測試權限認證機制之有效性。

八、定期檢視個人資料之存取權限設定。

九、於處理個人資料之電腦系統中安裝防毒、防駭軟體，並定期更新病毒碼。

十、對於電腦作業系統及相關應用程式之漏洞，定期安裝修補程式。

十一、對於具備存取權限之電腦或自動化處理設備，不得安裝檔案分享軟體。

十二、測試處理個人資料之資訊系統時，不使用真實個人資料，有使用真實個人資料之情形時，

明確規定使用程序。

十三、處理個人資料之資訊系統有變更時，確認其安全性並未降低。

十四、定期檢查處理個人資料資訊系統之使用狀況，及個人資料存取情形。

第 21 條

私立職業訓練機構執行本計畫各項程序及措施，應保存下列紀錄：

一、因應事故發生所採取之行為。

二、提供當事人行使之權利。

三、個人資料之維護及修正。

四、所屬人員權限之異動。

五、所屬人員違反權限之行為。

六、備份及還原之測試。

七、個人資料之交付及傳輸。

八、個人資料之刪除及銷毀。

九、存取個人資料者之資訊。

十、定期檢查處理個人資料之資訊。

十一、教育訓練。

十二、計畫稽核及改善措施之執行。

第 22 條

私立職業訓練機構業務終止後之個人資料處理，應刪除或銷毀儲存個人資料之媒介物中所儲存之資料，記錄並留存刪除或銷毀之方法、時間、地點及證明刪除或銷毀之方式。

第 23 條

私立職業訓練機構應定期檢查本計畫執行情形，並建立未落實執行之改善措施。

第 24 條

本辦法自發布日施行。