

法規名稱：著作權集體管理團體個人資料檔案安全維護管理辦法

發布日期：民國 110 年 12 月 21 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

- 1 著作權集體管理團體（以下簡稱集管團體）保有個人資料檔案者，應依其業務規模，配置管理之人員，規劃、訂定、修正及執行個人資料檔案安全維護計畫（以下簡稱本計畫）。
- 2 集管團體應於本辦法發布施行之日起六個月內完成本計畫之訂定，並應報請著作權專責機關備查。

第 3 條

- 1 本計畫應納入符合第四條至第十條規定之具體內容，並適時清查其所保有之個人資料檔案及其蒐集、處理或利用個人資料之作業流程，據以建立個人資料檔案清冊及處理個人資料作業流程說明文件。
- 2 集管團體應訂定本計畫之稽核機制，定期或不定期檢查本計畫執行狀況，確保本計畫之落實。
- 3 集管團體應隨時檢視所適用之個人資料保護法令及社會環境之變動，持續改善本計畫。

第 4 條

- 1 集管團體應適時評估其因蒐集、處理或利用個人資料可能面臨的法律或其他風險，並訂定個人資料被竊取、竄改、毀損、滅失或洩漏等事故發生後之應變機制，其內容應就下列事項為具體規定：
 - 一、採取適當之應變措施，包括降低及控制當事人損害之方式。
 - 二、查明事故發生原因及損害狀況，以適當方式通知當事人，並通報相關機關。
 - 三、研議改善或預防之措施。
- 2 集管團體遇有個人資料安全事故，將危及其正常營運，或個人資料被竊取、洩漏、竄改或其他侵害達一千筆以上者，應於發現事故後七十二小時內，依附表格式填列個人資料侵害事故通報及紀錄表，並以書面或電子郵件通報著作權專責機關。
- 3 著作權專責機關接受前項通報後，得依本法第二十二條至第二十五條規定，為適當之監督管理措施。

第 5 條

除法律另有規定外，集管團體應就下列個人資料蒐集、處理或利用事項，訂定具體程序或機制：

- 一、檢視個人資料之蒐集、處理、利用與本法第五條、第六條、第八條、第九條、第十九條第一項及第二十條第一項規定是否相符；依當事人同意而為特定目的外利用者，應確認已符合本法第七條第二項規定。

- 二、檢視個人資料是否正確，其正確性有爭議者，應視情形分別依本法第十一條第一項、第二項及第五項規定辦理。
- 三、對個人資料進行國際傳輸前，應檢視著作權專責機關有無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，同時對資料接收方為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、方式及當事人行使本法第三條所定權利等事項之監督。
- 四、於特定目的消失、期限屆滿或有違反本法其他規定而為個人資料之蒐集、處理或利用時，應主動或依當事人之請求，刪除或停止蒐集、處理、利用個人資料。
- 五、委託他人蒐集、處理或利用個人資料之全部或一部時，應有選任受託人之標準及評估機制，且應於委託契約或相關文件明確約定適當之監督方式，並確實執行。
- 六、當事人行使本法第三條所定之權利，應注意下列事項：
 - (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，並遵守本法第十三條有關處理期限之規定。
 - (四) 有本法第十條及第十一條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。

第 6 條

集管團體應考量業務性質、個人資料存取環境、個人資料傳輸之方法及個人資料之種類、數量等因素，採取適當之資訊安全、作業安全及設備安全之管理措施。

第 7 條

集管團體依前條規定採取之資訊安全管理措施，應包括下列事項：

- 一、個人資料有加密之必要者，應於蒐集、處理時，採取適當之加密措施。
- 二、個人資料有備份之必要者，應對備份資料採取適當之保護措施。
- 三、傳輸個人資料時，應依不同傳輸方式，採取適當之安全措施。
- 四、設定個人資料之存取權限，建立蒐集、處理或利用個人資料之電腦、相關設備或系統必要之控管機制，並定期確認其有效性。
- 五、建立因應惡意程式及系統漏洞所造成威脅之安全機制，並定期確認蒐集、處理或利用個人資料之電腦、相關設備或系統安全機制之有效性。
- 六、進行軟硬體測試時，應建立個人資料防護機制，如確有使用個人資料之必要時，應明確規定其使用之程序及安全管理方式。
- 七、定期檢視處理個人資料之資訊系統，檢查其使用狀況及存取個人資料之情形。

第 8 條

集管團體依第六條規定採取之作業安全管理措施，應包括下列事項：

- 一、與所屬人員約定保密義務。

- 二、對業務內容涉及個人資料蒐集、處理或利用之所屬人員，定期實施個人資料保護認知宣導及教育訓練。
- 三、依業務特性、內容及需求，設定所屬人員接觸個人資料之權限。
- 四、所屬人員離職後，應將其執行業務所持有之個人資料辦理交接，不得私自持有或繼續使用，並取消其存取權限。

第 9 條

集管團體依第六條規定採取之設備安全管理措施，應包括下列事項：

- 一、依電腦、自動化機器或其他儲存媒介物之特性及使用方式，建置適當之保護設備或技術。
- 二、所屬人員應妥善保管個人資料之媒介物。
- 三、針對存放儲存媒介物之環境，施以適當之進出管制措施。

第 10 條

- 1 集管團體執行本計畫時，應評估其必要性，保存下列紀錄：
 - 一、個人資料之蒐集、處理及利用紀錄。
 - 二、自動化機器設備之軌跡資料。
 - 三、其他落實執行本計畫之證據。
- 2 集管團體於業務終止後，其保有之個人資料應依下列方式處理：
 - 一、刪除、停止處理或利用個人資料者，記錄其方法、時間、地點及證明方式。
 - 二、移轉個人資料者，記錄其原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。
- 3 前項所稱業務終止，指著作權專責機關依著作權集體管理團體條例第四十八條規定命令集管團體解散，或集管團體依其章程規定決議解散。

第 11 條

本辦法自發布日施行。