內政部指定殯葬服務業個人資料檔案安全維護計畫管理辦法

修(訂)定日期：中華民國 110 年 11 月 30 日

◎訂定發布：104.10.05 內政部台內民字第 1041104670 號令訂定發布全文 22 條。

◎修正發布：110.11.30 內政部台內民字第 1100224326 號令訂定修正發布名稱及第 7.14 條條文；並增訂第 12~1.21~1 條條文(原名稱：殯葬服務業個人資料檔案安全維護管理辦法；新名稱：內政部指定殯葬服務業個人資料檔案安全維護管理辦法)。

◎【內政部指定殯葬服務業個人資料檔案安全維護管理辦法】，可至內政部「全國殯葬資訊入口網」下載，其網址為：(https://mort.moi.gov.tw)

第 1 條

本辦法依個人資料保護法(以下簡稱本法)第 27 條第 3 項規定訂定之。

第 2 條

本辦法所稱主管機關，在中央為內政部；在直轄市為直轄市政府；在縣(市)為縣(市)政府。

第 3 條

殯葬服務業應訂定個人資料檔案安全維護計畫(以下簡稱計畫)，以落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

前項所稱殯葬服務業，指依殯葬管理條例第 42 條規定經直轄市或縣（市）主管機關許可經營之殯葬設施經營業及殯葬禮儀服務業。

第 4 條

殯葬服務業訂定計畫時，得視其規模、特性、保有個人資料之性質及數量等事項，參酌第 6 條至第 20 條規定，訂定適當之安全維護管理措施。

前項計畫內容應包括下列項目，第二款相關項目必要時得整併之：

一、殯葬服務業之組織規模。

二、個人資料檔案之安全維護管理措施：

(一)配置管理之人員及相當資源。

(二)界定蒐集、處理及利用個人資料之範圍。

(三)個人資料之風險評估及管理機制。

(四)事故之預防、通報及應變機制。

(五)個人資料蒐集、處理及利用之內部管理程序。

(六)設備安全管理、資料安全管理及人員管理措施。

(七)認知宣導及教育訓練。

(八)資料安全稽核機制。
(九)使用紀錄、軌跡資料及證據保存。
(十)個人資料安全維護之整體持續改善。
(十一)業務終止後之個人資料處理方法。
殯葬服務業應將計畫公告於營業處所適當之處，如有網站者，並揭露於網站首頁，使其所屬人員及資料當事人均能知悉；計畫修正時，亦同。

第 5 條

殯葬服務業應於直轄市、縣(市)主管機關許可經營之日起 6 個月內將計畫報請該直轄市、縣(市)主管機關備查；本辦法施行前已經許可經營殯葬服務業，應於本辦法施行之日起 6 個月內將計畫報請備查。
殯葬服務業應參酌計畫執行狀況、技術發展及相關法令修正等因素，檢視所定計畫是否合宜，必要時應予以修正，修正後應於 15 日內將修正計畫報請備查。

第 6 條

殯葬服務業應配置適當管理人員及相當資源，負責規劃、訂定、修正與執行計畫或業務終止後個人資料處理方法等相關事項。

第 7 條

殯葬服務業應確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查所保有之個人資料現況。
殯葬服務業經清查發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理或利用等適當之處置，並留存相關紀錄至少 5 年。
殯葬服務業使用資通訊系統蒐集、處理或利用個人資料達 10000 筆以上者，應採取下列資訊安全措施：
一、使用者身分確認及保護機制。
二、個人資料顯示之隱碼機制。
三、網際網路傳輸之安全加密機制。
四、個人資料檔案與資料庫之存取控制及保護監控措施。
五、防止外部網路入侵對策。
六、非法或異常使用行為之監控及因應機制。
前項第 5 款及第 6 款所定措施，應定期演練及檢討改善。

第 8 條

殯葬服務業依殯葬管理條例第 56 條規定委託代為銷售生前殯葬服務契約、墓基及骨灰(骸)存放單位之公司或商業，為執行業務所蒐集、處理或利用之個人資料視為該殯葬服務業所持有，於蒐集、處

理或利用時應檢視是否符合特定目的之必要範圍，並接受該殯葬服務業監督。
前項監督措施應包含下列事項：
一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。
二、受託者就第 4 條第二項採取之措施。
三、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。
四、委託機關如對受託者有保留指示者，其保留指示之事項。
五、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。
第一項受委託之公司或商業應遵行之個人資料安全維護管理事項及委託業務終止後，其蒐集、處理或利用持有個人資料檔案之處置方式，殯葬服務業應於委託契約明定之。

第 9 條

殯葬服務業應依已界定蒐集、處理與利用個人資料之範圍及流程，分析評估可能發生之風險，並根據風險分析結果，訂定適當之管控措施。

第 10 條

殯葬服務業於蒐集個人資料應遵守本法第 8 條及第 9 條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求所屬人員確實辦理。

第 11 條

殯葬服務業所屬人員利用個人資料行銷時，應明確告知當事人其所屬公司或商業名稱。
殯葬服務業首次利用個人資料行銷時，應提供當事人免付費電話、免費回郵等免費表示拒絕接受行銷之方式。
殯葬服務業利用個人資料進行行銷，當事人表示拒絕接受行銷後，應立即停止利用其個人資料繼續行銷，並周知所屬人員、受委託之公司或商業。

第 12 條

殯葬服務業所蒐集之個人資料如需作特定目的外利用，應檢視是否符合本法第 20 條第一項但書規定，得為利用之情形。

第 12-1 條

中央主管機關依本法第 21 條規定，對殯葬服務業為限制國際傳輸個人資料之命令或處分時，殯葬服務業應通知所屬人員遵循辦理。
殯葬服務業將個人資料作國際傳輸者，應檢視是否受中央主管機關限制，告知當事人其個人資料所欲國際傳輸之區域，並對資料接收

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 3 條所定權利之相關事項。

第 13 條

殯葬服務業於當事人行使本法第 3 條規定之權利時，應依下列規定辦理：
一、提供聯絡窗口及聯絡方式。
二、確認是否為資料當事人之本人，或經其委託。
三、如認有本法第 10 條但書各款、第 11 條第二項但書或第三項但書得拒絕當事人行使權利之事由，應附理由通知當事人。
四、告知是否酌收必要成本費用及其收費基準，並遵守本法第 13 條處理期限規定。

本條文有附件

第 14 條

殯葬服務業為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故(以下簡稱個人資料事故)，應訂定下列應變、通報及預防機制：
一、個人資料事故發生後應採取之各類措施，包括：
　(一)控制當事人損害之方式。
　(二)查明個人資料事故後通知當事人之適當方式。
　(三)應通知當事人個人資料事故事實、所為因應措施及諮詢服務專線等內容。
二、個人資料事故發生後應受通報之對象及其通報方式。
三、個人資料事故發生後，其矯正預防措施之研議機制。
殯葬服務業遇有達 1000 筆以上之個人資料事故時，應於發現後 72 小時內將通報機關、發生時間、發生種類、發生原因及摘要、損害狀況、個人資料侵害可能結果、擬採取之因應措施、擬通知當事人之時間及方式、是否於發現個人資料外洩後立即通報等事項，以書面通報直轄市、縣(市)主管機關，並副知中央主管機關(書面通報格式如附件)。
直轄市、縣(市)主管機關對於重大個人資料事故，得依本法第 22 條規定對殯葬服務業之應變、通報及預防機制進行實地檢查，並視檢查結果為後續處置。中央主管機關認有必要時，得督導直轄市、縣(市)主管機關對於殯葬服務業之相關機制改善情形。

第 15 條

殯葬服務業對所保有之個人資料檔案，應採取必要適當之安全設備

或防護措施。
前項安全設備或防護措施應包含下列事項：
一、紙本資料檔案之安全保護設施及管理程序。
二、電子資料檔案存放之電腦、自動化機器相關設備、可攜式設備或儲存媒體，配置安全防護系統或加密機制。
三、個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片或其他存放媒介物需報廢汰換或轉作其他用途時，應採取適當防範措施，避免洩漏個人資料；若委託他人執行上開行為時，殯葬服務業應對受託人為適當之監督，並明確約定相關監督事項與方式。

第 16 條

殯葬服務業為確實保護個人資料之安全，應對其所屬人員採取下列措施：
一、依據業務作業需要，建立管理機制，設定所屬人員不同之權限，並定期確認權限內容之適當性及必要性。
二、檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。
三、要求所屬人員妥善保管個人資料之儲存媒介物，並約定保管及保密義務。
四、所屬人員離職時取消其識別碼，並應要求將執行業務所持有之個人資料辦理交接，不得攜離在外繼續使用，並應簽訂保密切結書。

第 17 條

殯葬服務業應訂定個人資料檔案安全維護查核機制，定期或不定期檢查計畫之執行情形。
前項定期檢查計畫之執行，每二年至少一次，並作成報告，其保存期限至少 5 年。

第 18 條

殯葬服務業應留存個人資料使用紀錄、自動化機器設備之軌跡資料或其他相關之證據資料。

第 19 條

殯葬服務業業務終止後，其保有之個人資料不得繼續使用，應依下列方式處理，並留存相關紀錄，其保存期限至少 5 年：
一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。
二、移轉：移轉之原因、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。
三、其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。

第 20 條

殯葬服務業對於個人資料蒐集、處理及利用須符合本法第 19 條及第 20 條相關規定，並定期或不定期對於所屬人員施以基礎認知宣導或專業教育訓練，使其明瞭個人資料保護相關法令規定、責任範圍及應遵守之相關管理措施。

第 21 條

直轄市、縣(市)主管機關應將殯葬服務業辦理個人資料檔案安全維護管理事項納入評鑑項目。

第 21-1 條

本辦法修正施行前，未訂定或已訂有計畫之殯葬服務業，應依本辦法規定訂定或修正，並於本辦法修正施行日起 6 個月內，將計畫報請直轄市、縣(市)主管機關備查。

第 22 條

本辦法自發布日施行。

第14條附件

<table>
<tr><td colspan="3">殯葬服務業個人資料事故通報及紀錄表</td></tr>
<tr><td>殯葬服務業者名稱
_____
通報機關
_____</td><td colspan="2">通報時間：　年　月　日　時　分
通報人：　　簽名(蓋章)
職稱：
電話：
Email：
地址：</td></tr>
<tr><td>發生時間</td><td colspan="2"></td></tr>
<tr><td rowspan="2">發生種類</td><td rowspan="2">□竊取
□竄改
□毀損
□滅失
□洩漏
□其他侵害情形</td><td>個人資料侵害之總筆數(大約)
_____</td></tr>
<tr><td>□一般個人資料 _____筆
□特種個人資料 _____筆</td></tr>
<tr><td>發生原因及摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個人資料侵害可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於發現個人資料外洩後七十二小時內通報</td><td colspan="2">□ 是　　□否，理由：</td></tr>
</table>

備註：特種個人資料，指有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料；一般個人資料，指特種個人資料以外之個人資料。