

內政部指定宗教團體個人資料檔案安全維護管理辦法總說明

個人資料保護法（以下簡稱本法）第二十七條規定：「非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。」鑑於宗教團體為事務運作需要，蒐集持有之個人資料，為防止個人資料被竊取、竄改、毀損、滅失或洩漏，宗教團體對所保有之個人資料檔案應採行適當之安全措施，爰依本法第二十七條第三項規定授權，並參酌本法施行細則第十二條規定，訂定內政部指定宗教團體個人資料檔案安全維護管理辦法（以下簡稱本辦法），以資宗教團體遵循，其要點如下：

- 一、本辦法之訂定依據。（第一條）
- 二、本辦法之主管機關。（第二條）
- 三、宗教團體之定義。（第三條）
- 四、宗教團體應訂定個人資料檔案安全維護計畫及業務終止後個人資料處理方法（以下簡稱本計畫及處理方法）、訂定內容及訂定時限。（第四條）
- 五、宗教團體應配置適當管理人員及提供相當資源，以執行本計畫及處理方法，及公告個人資料保護管理政策等事項。（第五條）
- 六、個人資料之範圍界定及個人資料檔案現況之盤點、業務流程之風險分析與管控，及相關侵害事故之應變等事項。（第六條至第八條）
- 七、宗教團體所屬人員為執行業務蒐集個人資料之規範、宗教團體所蒐集持有及應遵守告知義務等事項。（第九條及第十條）
- 八、宗教團體國際傳輸個人資料時應遵循事項。（第十一條）
- 九、宗教團體對於當事人行使本法第三條規定之權利時採取之措施。（第十二條）
- 十、宗教團體對所保管之個人資料檔案應採取必要適當之防護設施，並應對所屬人員有適度之管理措施。（第十三條及第十四條）

- 十一、宗教團體使用資通訊系統蒐集、處理或利用個人資料時應採取之資訊安全措施。（第十五條）
- 十二、宗教團體應定期或不定期對所屬人員進行教育宣導。（第十六條）
- 十三、本計畫及處理方法之稽核、使用紀錄留存及檢討改善等事項。（第十七條至第十九條）
- 十四、宗教團體委託他人蒐集、處理或利用個人資料時，應對受託者為適當之監督。（第二十條）
- 十五、宗教團體因解散或經主管機關廢止登記後，其保有個人資料之處理方式。（第二十一條）
- 十六、本辦法施行前之宗教團體，應訂定本計畫及處理方法，並於一定期間報備查。（第二十二條）
- 十七、本辦法施行日期。（第二十三條）

內政部指定宗教團體個人資料檔案安全維護管理辦法

條 文	說 明
<p>第一條 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。</p>	<p>本辦法訂定依據。</p>
<p>第二條 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。</p>	<p>本辦法主管機關。</p>
<p>第三條 本辦法所稱宗教團體，指已完成寺廟登記之寺廟或宗教財團法人。</p>	<p>本條定明本辦法之適用對象，宗教社團（法人）另依人民團體相關規定辦理。</p>
<p>第四條 宗教團體應訂定個人資料檔案安全維護計畫及業務終止後個人資料處理方法（以下簡稱本計畫及處理方法），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。</p> <p>宗教團體依前項規定訂定本計畫及處理方法時，應視其業務規模、特性、保有個人資料之性質及數量等事項，參酌第五條至第二十一條規定，訂定包含下列各款事項之適當安全維護管理措施；必要時，第二款各目事項得整併之：</p> <ol style="list-style-type: none"> 一、宗教團體之組織規模及特性。 二、個人資料檔案之安全管理措施： <ol style="list-style-type: none"> （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）個人資料安全維護稽核機制。 （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 	<ol style="list-style-type: none"> 一、依個人資料保護法（以下簡稱本法）第二十七條第二項規定，於第一項指定之非公務機關應訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。 二、本辦法規定之相關組織及程序要求，宗教團體應定明於個人資料檔案安全維護計畫及業務終止後個人資料處理方法（以下簡稱本計畫及處理方法）內，並定期檢視及配合相關法令修正。 三、參照本法施行細則第十二條第二項規定意旨，所採行之安全措施與所欲達成之個人資料保護目的間，具有適當比例為原則。爰第二項規定宗教團體得參酌其業務規模、特性、保有個人資料之性質及數量等事項，參考第五條至第二十二條及本法施行細則第十二條第二項規定，訂定適宜並符合比例原則之安全措施，據以執行，另保留彈性空間，得依個別情況於必要時整併第二項第二款各目之相關事項。 四、第三項定明宗教團體應於完成登記之日起六個月內訂定本計畫及處理方法，並報請中央或直轄市、縣（市）主管機關備查。

<p>持續改善。</p> <p>(十一) 業務終止後之個人資料處理方法。</p> <p>第一項之本計畫及處理方法，宗教團體應於完成登記之日起六個月內報請其主管機關備查。</p>	
<p>第五條 宗教團體應配置適當管理人員及相當資源，負責規劃、訂定、修正及執行本計畫及處理方法等相關事項，並定期向宗教團體負責人或管理組織提出報告。</p> <p>宗教團體應訂定個人資料保護管理政策，將蒐集、處理及利用個人資料之特定目的、法律依據及其他相關保護事項，公告於宗教團體處所或其他適當處所；如有網站者，並揭露於網站首頁，使其所屬人員及個人資料當事人均能知悉。</p>	<p>一、第一項規定宗教團體應指派配置適當管理人員，負責本計畫及處理方法之規劃、訂定、修正及執行等事宜，並提供適當之資源協助，以為確保個人資料維護安全措施發揮效能。另本法第四十八條第四款及第五十條規定，對違反本法第二十七條第一項或未依同條第二項訂定計畫或業務終止後個人資料處理方法之非公務機關之代表人得併同處罰。爰規定負責本計畫及處理方法之管理人員須定期向宗教團體負責人或管理組織（如：董事會或管理委員會等）提出報告，促使負責人或管理組織能據以監督本計畫及處理方法之執行，落實對個人資料保護之工作。</p> <p>二、為能讓宗教團體所屬人員明瞭個人資料保護之重要性，第二項規定宗教團體應將個人資料保護管理政策及蒐集、處理及利用個人資料之特定目的、法律依據及其他相關保護，公告於宗教團體處所或其他適當處所，以供所屬人員遵循，更可使當事人知曉宗教團體保護個人資料之相關事項，俾保護自身權益。</p>
<p>第六條 宗教團體應依個人資料保護相關法令，定期查核確認所保有之個人資料現況，界定其納入本計畫及處理方法之範圍。</p>	<p>宗教團體蒐集個人資料應定期清查所蒐集保有之個人資料是否符合所界定之本計畫及處理方法範圍。</p>
<p>第七條 宗教團體應依前條界定之個人資料範圍及其蒐集、處理、利用個人資料之流程，評估可能產生之個人資料風險，並根據風險評估之結果，訂定適當之管控機制。</p>	<p>定明宗教團體應參酌整體運作狀況，就已界定個人資料之範圍與蒐集、處理及利用個人資料流程，分析評估可能發生之風險，並針對該可能發生之風險，採取必要之防範與管控措施，避免個人資料被竊取、竄改、洩漏、毀損、滅失或濫用。</p>
<p>第八條 宗教團體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</p>	<p>一、本法第十二條規定，非公務機關所持有之個人資料發生被竊取、洩漏、竄改或其他侵害事故者，應查</p>

<p>訂定下列應變、通報及預防機制：</p> <p>一、個人資料事故發生後應採取之各類措施，包括：</p> <p>（一）控制當事人損害之方式。</p> <p>（二）查明個人資料事故後通知當事人之適當方式。</p> <p>（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。</p> <p>二、個人資料事故發生後應受通報之對象及其通報方式。</p> <p>三、個人資料事故發生後，其矯正預防措施之研議機制。</p> <p>宗教團體遇有達五千筆以上之個人資料事故時，應於發現後七十二小時內將通報機關、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，以書面通報其主管機關。如為直轄市、縣(市)主管機關接獲通報，並應副知中央主管機關(書面通報格式如附件)。</p> <p>主管機關對於重大個人資料事故，得依本法第二十二條規定對宗教團體之應變、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)主管機關對於宗教團體之相關機制改善情形。</p>	<p>明後以適當方式通知當事人。爰第一項規定宗教團體在本計畫及處理方法中應訂定應變機制及其必要作為之相關事項，在發生個人資料被竊取等侵害事故時，得迅速遵循處理，以保護當事人之權益。</p> <p>二、第二項參考殯葬服務業個人資料檔案安全維護管理辦法第十四條規定，並考量宗教團體組織規模差異，爰定明宗教團體遇有達五千筆以上之個人資料被竊取、洩漏、竄改或其他侵害之重大個人資料事故時，負通報義務。並依行政院一百一十年二月三日「行政機關落實個人資料保護執行聯繫會議」第一次會議決議，定明事故通報時點及應通報事項。</p> <p>三、為調查事故發生後，是否係宗教團體所採取保護安全措施不足導致，第三項定明中央及地方主管機關對於重大個人資料事故得採取之措施及後續行政檢查規定。</p>
<p>第九條 宗教團體所屬人員為執行業務而蒐集、處理一般個人資料時，應檢視是否符合本法第十九條之要件；利用時，應檢視是否符合蒐集之特定目的必要範圍；為特定目的外之利用時，應檢視是否符合本法第二十條第一項但書情形。</p>	<p>定明宗教團體所屬人員執行業務蒐集個人資料時，應遵守相關法定要件及程序。</p>
<p>第十條 宗教團體蒐集個人資料，應遵守本法第八條及第九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。</p>	<p>為尊重當事人能知曉其個人資料被蒐集之狀況，本法第八條及第九條規定資料蒐集者有告知義務。爰規定宗教團體，應區分個人資料蒐集方式為直接蒐集或間接蒐集，分別訂定告知之方法、內容及相關注意事項，以便所屬人員在辦理業務時能據以執行。</p>
<p>第十一條 中央主管機關依本法第二十</p>	<p>一、第一項規定中央主管機關依本法第</p>

<p>一條規定，對宗教團體為限制國際傳輸個人資料之命令或處分時，宗教團體應通知所屬人員遵循辦理。</p> <p>宗教團體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，並告知當事人其個人資料所欲國際傳輸之區域，且對資料接收方為下列事項之監督：</p> <p>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。</p> <p>二、當事人行使本法第三條所定權利之相關事項。</p>	<p>第二十一條規定所為之命令或處分，宗教團體應通知所屬人員知曉並遵照辦理。</p> <p>二、第二項規定宗教團體將個人資料作國際傳輸者，應檢視是否受中央主管機關依本法第二十一條規定之命令或處分限制，並且告知個人資料所欲國際傳輸之區域，同時對資料接收方為相關之監督。</p>
<p>第十二條 宗教團體於個人資料當事人行使本法第三條規定之權利時，應依下列規定辦理：</p> <p>一、提供聯絡窗口及聯絡方式。</p> <p>二、確認為個人資料當事人本人，或經其委託者。</p> <p>三、認有本法第十條但書各款、第十一條第二項但書或第三項但書規定得拒絕當事人行使權利之事由，應附理由通知當事人。</p> <p>四、有收取必要成本費用者，應告知當事人收費基準。</p> <p>五、遵守本法第十三條有關處理期限規定。</p>	<p>依本法第三條規定，當事人就其個人資料得行使查詢或請求閱覽、製給複製本、補充或更正、停止蒐集、處理或利用及刪除其個人資料等權利，且宗教團體除有本法第十條但書、第十一條第二項但書或第三項但書規定得拒絕當事人行使權利之情形外，應於本法第十三條規定期間內准駁當事人之請求，爰本條規定明宗教團體應辦理事項，以利資料當事人行使權利。</p>
<p>第十三條 宗教團體對所蒐集保管之個人資料檔案，應採取必要適當之安全設備或防護措施。</p> <p>前項安全設備或防護措施，應包含下列事項：</p> <p>一、紙本資料檔案之安全保護設施。</p> <p>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。</p> <p>三、存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片或其他存放媒介物報廢汰換或轉作其他用途時，應採取適當之銷毀或防範措施，避免洩漏個人資料；委託他人執行者，宗教團體對受託者之監督依第二十條規定辦理。</p>	<p>為確保宗教團體所保管之個人資料檔案不被竊取、竄改、毀損、滅失或洩漏，爰第一項規定宗教團體得視其性質、資料儲存之媒介物及其數量等，於所訂本計畫及處理方法中採取必要且適當之安全設備或防護措施。第二項並規定安全設備或防護措施應包括事項，例如：對紙本資料之保護應採用堅固之保險箱或櫥櫃；電腦設備應設置防火牆及防毒程式、對複製或上傳檔案行為予以管控、制定紙本資料之銷毀程序、磁碟、磁帶、光碟片、微縮片、積體電路晶片及其他存放個人資料之媒介物需報廢汰換或轉作其他用途時，應確實刪除所存放之個人資料檔案或防範洩漏個人資料等。</p>
<p>第十四條 宗教團體為確實保護個人資</p>	<p>一、宗教團體與所屬人員，不論是何種</p>

<p>料之安全，應對其所屬人員採取適度管理措施。</p> <p>前項管理措施，應包含下列事項：</p> <ol style="list-style-type: none"> 一、依據業務需求，適度設定所屬人員不同之權限控管其接觸個人資料之情形，並定期檢視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、所屬人員異動或離職時，應將執行業務所持有之個人資料辦理交接，不得在外繼續使用，並應簽訂保密切結書。 	<p>法律關係，宗教團體都必須避免個人資料之保管及處理發生弊端，導致侵害當事人權益情事，爰第一項規定應於所訂本計畫及處理方法中，對所屬人員採取必要且適當之管理措施。</p> <ol style="list-style-type: none"> 二、第二項規定宗教團體應根據業務性質，檢視容易發生問題之處，預先予以防範。例如：與業務無關人員不得任意接觸資料、授予必要利用個人資料人員不同等級之權限、所屬人員在個人資料蒐集、處理及利用流程中有無漏洞、約束規範嚴密保管個人資料檔案及所屬人員工作異動時，所持有之個人資料如何交接與保密切結等事項。
<p>第十五條 宗教團體使用資通訊系統蒐集、處理或利用個人資料達一萬筆以上者，應採取下列資訊安全措施：</p> <ol style="list-style-type: none"> 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。 <p>前項第五款及第六款所定措施，應定期演練及檢討改善。</p>	<ol style="list-style-type: none"> 一、依據行政院一百十年二月三日會議決議事項，非公務機關使用資通訊系統蒐集、處理或利用個人資料，為避免使用者個人資料於使用資通訊服務時被竊取、洩漏、竄改或其他侵害事故發生，並參酌製造業及技術服務業個人資料檔案安全維護管理辦法第二條規定及行政院資通安全處建議採取之資訊安全措施，於第一項定明宗教團體使用資通訊系統保有個人資料筆數達一萬筆以上者，應訂定之資訊安全措施，以落實保護個人資料。另參考資通安全責任等級分級辦法附表十資通系統防護基準，針對六類資訊安全措施之實作說明如下： <ol style="list-style-type: none"> (一) 系統應建立帳號管理機制，包含帳號申請、建立、修改、啟用、停用及刪除程序，並執行身分驗證管理，如身分驗證資訊不以明文傳輸、密碼複雜度或帳號鎖定機制等。 (二) 系統界面呈現個人資料時，應以適當且一致性之隱碼或遮罩處理，以避免過多且非必要之個人資料揭露，可參考 CNS 二九一九一「資訊技術—安全技術—部分匿名及部分去連結鑑別之要求事

	<p>項」國家標準。</p> <p>(三) 個人資料傳輸時，應採用傳輸加密機制，如採用加密傳輸通道、使用公開、國際機構驗證且未遭破解之演算法。</p> <p>(四) 儲存於電子媒體及資料庫之個人資料，應適當加密保護，並提供使用者識別、鑑別及身管理，並採用最小權限原則進行存取控制管理。</p> <p>(五) 針對外部入侵之防禦，應採用適當資安控制措施建立防禦縱深，包括防毒軟體、防火牆、入侵偵測與防禦系統，及應用程式防火牆等。</p> <p>(六) 針對系統或個人資料檔案之存取，應確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件，且應留存系統相關日誌紀錄並定期檢視，或設置適當監控及異常行為預警機制。</p> <p>二、隨網路科技之進步，個人資料遭外部網路入侵或非法或異常使用行為損害情形層出不窮，爰第二項定明針對第一項第五款及第六款所定措施，宗教團體應定期進行演練及檢討改善。</p>
<p>第十六條 宗教團體應定期或不定期對於所屬人員施以基礎個人資料保護認知宣導及教育訓練，使其明瞭相關法令之要求、所屬人員之責任範圍與各種個人資料保護事項之機制、程序及措施。</p>	<p>定明宗教團體應定期或不定期對所屬人員施以認知宣導或教育訓練，以使所屬人員能充分認知個人資料保護相關法令及責任範圍，避免發生違法情事。</p>
<p>第十七條 宗教團體為確保本計畫及處理方法之落實，應依其業務規模及特性，衡酌資源之合理分配，訂定個人資料安全維護稽核機制，並指定適當人員每半年至少進行一次本計畫及處理方法執行情形之檢查。</p> <p>前項檢查結果應向宗教團體負責人或管理組織提出報告，並留存相關紀錄，其保存期限至少五年。</p> <p>宗教團體依第一項檢查結果發現本計畫及處理方法不符法令或有不符法令之虞者，應即改善。</p>	<p>一、第一項、第二項規定宗教團體訂定之本計畫及處理方法應包含安全稽核機制，由適當管理人員檢查本計畫及處理方法是否落實執行，並應將檢查結果報告宗教團體負責人或管理組織，並須留存相關紀錄至少五年。</p> <p>二、第三項規定檢查結果發現本計畫及處理方法不符法令者，宗教團體應作必要之改善。</p>

<p>第十八條 宗教團體執行本計畫及處理方法所定各種個人資料保護機制、程序及措施，應記錄其個人資料使用情況，留存軌跡資料或相關證據。</p> <p>宗教團體依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄：</p> <ol style="list-style-type: none"> 一、刪除、停止處理或利用之方法、時間或地點。 二、將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間、地點，及該對象蒐集、處理或利用之合法依據。 <p>前二項之軌跡資料、相關證據及紀錄，應至少留存五年。但法令另有規定或契約另有約定者，不在此限。</p>	<p>第一項定明宗教團體應記錄其個人資料使用情況，並留存軌跡資料或相關證據；另於第二項規定依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料時，亦應留存相關紀錄；且於第三項規範上述軌跡資料、相關證據及紀錄，除法令另有規定或契約另有約定者外，應至少留存五年。</p>
<p>第十九條 宗教團體應隨時參酌業務及本計畫及處理方法執行狀況、社會輿情、技術發展及相關法規訂修等因素，檢討所定本計畫及處理方法，必要時予以修正；修正時，應於十五日內將修正後之本計畫及處理方法報請其主管機關備查。</p>	<p>由於科技發展不斷進步，社會活動型態亦隨時改變，爰規定宗教團體應注意媒體對個人資料侵害或保護事件相關報導，並配合個人資料保護法令之訂修，隨時檢討所訂本計畫及處理方法。如有不合時宜之處，應立即修正本計畫及處理方法，以落實保護個人資料。</p>
<p>第二十條 宗教團體委託他人蒐集、處理或利用個人資料之全部或一部時，應依本法施行細則第八條規定為適當監督。</p> <p>宗教團體為執行前項監督，應與受託者明確約定相關監督事項及方式。</p>	<p>依本法施行細則第八條之規定，委託他人蒐集、處理或利用個人資料時，委託者應為適當之監督，避免受託者有違反本法情事發生，爰第一項定明宗教團體委託他人蒐集、處理或利用個人資料之全部或一部時，應為適當之監督，並於第二項規定與受託者約定相關監督事項與方式。</p>
<p>第二十一條 宗教團體因解散或經主管機關廢止登記後，其保有之個人資料不得繼續使用，應依下列方式處理，並將相關紀錄報送其主管機關，由其主管機關保存至少五年：</p> <ol style="list-style-type: none"> 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。 	<ol style="list-style-type: none"> 一、宗教團體解散或經主管機關廢止登記後，自不得再繼續持有使用個人資料，應作妥善處置。爰規定此類宗教團體應將所保有之個人資料予以銷毀、移轉或其他刪除、停止處理或利用等方式處理，並將相關紀錄報送主管機關保存一定時間。 二、宗教團體在銷毀、移轉或其他刪除、停止處理或利用個人資料過程中，亦宜保存執行方法、時間、地點、執行人員、接受移轉個人資料之對象及合法移轉個人資料之法規依據等資料，以便日後舉證。

<p>第二十二條 本辦法發布施行前，未訂定本計畫及處理方法之宗教團體，應依本辦法規定訂定，並於本辦法發布施行日起六個月內，將本計畫及處理方法報請其主管機關備查。</p>	<p>規範本辦法施行前之宗教團體，應依本辦法訂定本計畫及處理方法，並於一定期間內報備查。</p>
<p>第二十三條 本辦法自發布日施行。</p>	<p>本辦法施行日期。</p>

附件

個人資料事故通報及紀錄表		
宗教團體名稱 _____	通報時間： 年 月 日 時 分	通報人： 簽名(蓋章)
通報機關 _____	職稱：	電話：
	Email：	地址：
發生時間		
發生種類	<input type="checkbox"/> 竊取	個人資料侵害之總筆數(大約) _____
	<input type="checkbox"/> 竄改	
	<input type="checkbox"/> 毀損	<input type="checkbox"/> 一般個人資料_____筆
	<input type="checkbox"/> 滅失	<input type="checkbox"/> 特種個人資料_____筆
	<input type="checkbox"/> 洩漏	
	<input type="checkbox"/> 其他侵害情形	
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七十二小時內通報	<input type="checkbox"/> 是 <input type="checkbox"/> 否，理由	

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。

說明：依據第八條第二項規定，定明宗教團體遇有達五千筆以上之個人資料侵害事故發生，應依本表格式通報主管機關，如為直轄市、縣（市）主管機關，並應副知中央主管機關。