

(營造業等 6 行業)個人資料管理外部稽核表

(機關名稱)檢查人員： 檢查日期： 年 月 日

稽核項目	辦理情形			發現說明
	是	否	不適用	
一、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				
(一)內政部指定營建類非公務機關個人資料檔案安全維護管理辦法(以下簡稱安維辦法)第 3 條之納管對象？ 請勾選事業類別： <input type="checkbox"/> 營造業 <input type="checkbox"/> 不動產開發業 <input type="checkbox"/> 建築師事務所 <input type="checkbox"/> 公寓大廈管理維護公司 <input type="checkbox"/> 都市更新業務財團法人 <input type="checkbox"/> 其他經中央主管機關公告指定者				
(二)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)？				
(三)代表人、管理人或其他有代表權人，及所採取的監督措施				
二、管理人員及資源				
(一)至少配置 1 名管理人員及相當資源，負責規劃、訂定、修正及執行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)等相關事項，並定期向負責人提出報告？				
(二)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，公告於營業處所或主事務所適當之處；如有網站者，並揭露於網站首頁，使其所屬人員及個人資料當事人均能知悉？				

稽核項目	辦理情形			發現說明
	是	否	不適用	
三、個人資料之範圍界定與清查				
一、定期清查保有之個人資料現況 二、確認保有之個人資料所應遵循適用之個人資料保護相關法令現況				
四、風險評估及管理機制				
(一) 就已界定之個人資料範圍及蒐集、處理、利用個人資料之流程，評估可能產生之風險？				
(二) 根據風險評估之結果，依風險等級訂定適當之管控措施？				
五、事故之預防、通報及應變機制				
(一) 已採取適當之應變措施，以控制個人資料事故對當事人之損害，並通報內部有關單位？(通報內部)				
(二) 已查明個人資料事故之狀況，並以適當方式通知當事人有關「個人資料被侵害之事實」及「已採取之因應措施」及所提供之諮詢服務專線 相關資訊？				
(三) 已依據風險評估結果或個人資料事故研議 事前預防 或 事後預防 機制，避免類似個人資料事故再次發生？				
(四) 針對重大個人資料事故達1000筆以上，於發現後72小時內，填寫「附件個人資料事故通報及紀錄表」以書面通報主事務所所在地之地方機關或財團法人主管機關？ 如地方機關接獲通報副知內政部？(通報外部)				
(五) 配合個人資料保護法行政檢查				
六、個人資料蒐集、處理及利用之內部管理程序				
(一) 屬個人資料保護法第六條所定特				

稽核項目	辦理情形			發現說明
	是	否	不適用	
種個人資料者，已檢視其特定目的及符合相關法令之要件？				
(二)已檢視所屬人員進行一般個人資料之蒐集、處理，應符合個人資料保護法第十九條規定應具有特定目的及法定要件？				
(三)已檢視所屬人員進行一般個人資料之利用，符合個人資料保護法第二十條規定，於蒐集之特定目的必要範圍內為之？特定目的外之利用，符合個人資料保護法第二十條第一項但書規定？				
(四)利用個人資料為行銷，當事人表示拒絕行銷後，所屬人員立即停止利用其個人資料行銷，且周知所屬人員，並至少於首次行銷時，提供當事人免費表示拒絕接受行銷之方式？				
(五)所屬人員於蒐集、處理或利用過程中，檢視個人資料正確？有不正確時，主動更正或補充？其正確性有爭議者，依個人資料保護法第十一條第二項規定辦理？				
(六)所屬人員蒐集個人資料，遵守個人資料保護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？ 告知後同意符合個人資料保護法第7條規定？				
(七)內政部依個人資料保護法第21條規定，對本公司為限制國際傳輸個人資料之命令或處分時，已通知所屬人員遵循辦理？ 本公司將個人資料作國際傳輸者，已檢視有否受中央主管機關限制，並告				

稽核項目	辦理情形			發現說明
	是	否	不適用	
<p>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>1、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>2、當事人行使個人資料保護法第三條所定權利之相關事項？</p>				
<p>(八)對於個人資料當事人行使個人資料保護法第三條規定之權利時，依下列規定辦理？</p> <p>1、提供聯絡窗口及聯絡方式。</p> <p>2、確認為個人資料當事人本人，或經其委託者。</p> <p>3、認有個人資料保護法第十條但書各款、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時，應附理由通知當事人。</p> <p>4、有收取必要成本費用者，應告知當事人收費基準。</p> <p>5、遵守個人資料保護法第十三條有關處理期限之規定。</p>				
<p>(九)個人資料蒐集之特定目的消失或期限屆滿時，依個人資料保護法第十一條第三項規定主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。</p>				
<p>(十)委託他人蒐集、處理或利用個人資料之全部或一部時，受託人依個人資料保護法施行細則第八條規定為適當之監督？本公司與受託人明確約定相關監督事項及方式？</p> <p>委託他人執行媒介物報廢、汰換或轉作其他用途時，對受託人進行監督？</p>				
七、資料安全管理措施				
<p>(一)運用電腦或自動化機器相關設備蒐集、處理或利用個人資料時，訂定</p>				

稽核項目	辦理情形			發現說明
	是	否	不適用	
各類設備或儲存媒體之使用規範？				
(二)針對所保有之個人資料內容，如有加密之需要，於蒐集、處理或利用時，採取適當之加密機制？				
(三)作業過程有備份個人資料之需要時，該備份資料比照原件，依個人資料保護法規定予以保護之？				
(四)針對存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物，於報廢、汰換或轉作其他用途時，採取適當防範措施？				
(五)委託他人執行個人資料報廢、汰換或轉作其他用途者，應比照前項規定，採取適當防範措施？				
八、資通訊系統 (安維辦法第15條)				
使用資通訊系統蒐集、處理或利用個人資料，且其資料庫保有個人資料數量達五千筆以上者，採取下列措施？ (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？ (七)針對第五款防止外部網路入侵對策，定期演練及檢討改善？ (八)針對第六款非法或異常使用行為之監控及因應機制，定期演練及檢討改善？				
九、環境及實體設備安全				
(一)、依據作業內容之不同，實施適宜之進出管制方式？				
(二)訂定媒介物之管制方式，並檢視其保管情形？				

稽核項目	辦理情形			發現說明
	是	否	不適用	
(三)針對不同媒介物存在之環境，建置適度之保護設備或技術？				
十、人員安全				
(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存有個人資料之媒介物，並約定保管及保密義務？				
(四)所屬人員異動或離職時，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？				
十一、認知宣導及教育訓練				
(一)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？				
(二)所屬人員完成訓練或取得宣導資料後，已明瞭個人資料保護相關法令之要求、所屬人員之責任範圍、各種個人資料保護事項之作業程序及應遵守之相關管理措施。				
十二、資料安全稽核機制				
(一)依本公司業務規模及特性，衡酌經營資源之合理分配，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？				
(二)將前項檢查結果應向負責人提出報告，並留存相關紀錄，其保存期限至少五年？				
(三)稽核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，				

稽核項目	辦理情形			發現說明
	是	否	不適用	
立即改善？				
<p>(四)非公務機關是否依中央流行疫情指揮中心「防疫個人資料稽核指引」第3條至第5條規定，將防疫個人資料稽核併入其現行之個人資料安全維護稽核；每年自行辦理防疫個人資料稽核作業，並製作包含個資管理制度之執行狀況以及稽核後改善計畫之稽核報告？</p> <p>地方機關依「防疫個人資料稽核指引」第3條至第5條規定，應督導非公務機關辦理個人資料安全維護稽核及改善情形。稽核重點應包括：蒐集告知義務（個人資料保護法第8條及第9條）、防疫個資保存期限（自蒐集日起28日內）、辦理安全維護事項（安維辦法第5條至第23條）、留存防疫個資之銷毀紀錄(安維辦法第23條)。</p> <p>依據嚴重特殊傳染性肺炎中央流行疫情指揮中心（以下簡稱中央流行疫情指揮中心）111年8月3日肺中指字第1114300137號函辦理。</p>				
十三、使用紀錄、軌跡資料及證據保存				
(一)依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，記錄其個人資料使用情況，留存軌跡資料或相關證據？				
<p>(二)證據或紀錄之保存期限？</p> <p>1、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>2、稽核檢查結果應向負責人提出報告，並留存相關紀錄，其保存期限至少五年。</p> <p>3、個人資料業務終止後，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，其保存期限至少五年。</p>				

稽核項目	辦理情形			發現說明
	是	否	不適用	
十四、整體持續改善				
(一)依公司(商號)之規模、特性、保有個人資料之性質及數量等事項，訂定適當之本計畫及處理方法？				
(二)隨時參酌業務及本公司所訂安維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，檢討所定安維計畫及處理方法，必要時予以修正？於規定時間內將修正後之安維計畫及處理方法報請所在地直轄市、縣(市)主管機關備查？				
十五、個人資料業務終止後個人資料處理方法				
針對個人資料之銷毀、移轉、刪除、停止處理或利用，其處理方式及應記載事項為？ (一)個資銷毀之 1 處理方式 2 應記載事項為：銷毀之方法、時間、地點及證明銷毀之方式。				
(二)個資移轉之 1. 處理方式 2. 應記載事項為：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)刪除、停止處理或利用個人資料之 1. 處理方式 2. 應記載事項為：刪除、停止處理或利用之方法、時間或地點。				
(四)委託他人執行個人資料報廢、汰換或轉作其他用途者，是否遵守本項規定辦理？				

公司名稱：

個人資料專責管理人簽章：