

## 記帳士個人資料管理內部自主稽核表

稽核項目	辦理情形			發現說明
	是	否	不適用	
<b>一、專責人員及資源</b>				
(一)是否至少配置1名專責人員，負責規劃、訂定、修正與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等相關事項，並定期向負責人提出報告？				
(二)是否訂定個人資料保護管理政策，並公告於4事務所適當之處或網站，使其所屬人員及個人資料當事人均能知悉？				
<b>二、個人資料之範圍界定</b>				
是否定期查核確認所保有之個人資料現況，並界定納入計畫及處理方法之範圍？				
<b>三、風險分析及管理機制</b>				
是否就所界定之個人資料範圍及其蒐集、處理、利用個人資料之流程，評估可能產生之個資風險，並根據風險評估之結果，訂定適當之管控機制？				
<b>四、預防個人資料事故及通報措施</b>				
(一) 是否已建立並執行個人資料事故之應變、通報及預防機制，包括個人資料事故發生後應採取之各類措施、應受通報之對象及其通報方式及改善預防措施之研議機制？				
(二)所建立的應變措施，是否包含控制當事人損害之方式、查明個人資料事故後通知當事人之適當方式及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？				
(三) 是否訂定並執行個人資料事故時，應於發現後72小時內，以書面通報財政部之機制？				
<b>五、個人資料蒐集、處理及利用之內部管理程序</b>				
(一)是否告知所屬人員，執行業務蒐集、處理一般個人資料時，應檢視是否符合個人資料保護法（以下簡稱本法）第19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				

稽核項目	辦理情形			發現說明
	是	否	不適用	
的外之利用時，應檢視是否符合本法第20條第1項但書情形？				
(二)蒐集個人資料時，是否遵守本法第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？				
(三) 是否訂定並執行維護個人資料正確性之方式				
(四) 是否訂定並執行定期確認保有個人資料之目的及期限，並留存銷毀、移轉、刪除、停止處理或利用個資相關紀錄。				
(五) 是否訂定並執行委託他人蒐集、處理或利用個人資料之全部或一部時，對受託者將為適當之監督，並明確約定相關監督事項及方式。				
(六) 是否訂定並執行將當事人個人資料作國際傳輸者，將檢視是否受財政部限制，並告知當事人其個人資料所欲國際傳輸之區域，及對資料接收方為下列事項之監督: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。2.當事人行使個人資料保護法第3條所定權利之相關事項。				
<b>六、個人資料管理措施</b>				
(一)是否依據業務需求，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)是否檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程及其負責人員？				
(三)是否明定所屬人員應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)是否明定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，並簽訂保密切結書？				
(五)使用資通訊系統蒐集、處理或利用消費者個人資料達1萬筆以上時，是否採取使用者身分確認及保護機制、個人資料顯示之隱碼機制、網際網路傳輸之安全加密機制、個人資料檔案與資料庫之存取控制及保護監控措施？				

稽核項目	辦理情形			發現說明
	是	否	不適用	
(六)使用資通訊系統蒐集、處理或利用消費者個人資料達1萬筆以上時，是否有防止外部網路入侵對策及非法或異常使用行為之監控及因應機制，並進行定期演練及檢討改善？				
<b>七、人員管理措施</b>				
(一)是否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)所屬人員是否均已完成訓練或取得宣導資料，並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？				
<b>八、設備安全管理</b>				
(一)所蒐集保管之個人資料檔案，是否就存放或處理現有各種不同個人資料媒體型態（包含紙本、電腦、自動化機器或其他存放媒介物）之設備採取必要適當之安全設備或防護措施？				
(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，是否配置安全防護系統或加密機制？				
(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，是否採取適當之銷毀或防範措施？				
(四)委託他人蒐集、處理或利用個人資料之全部或一部，或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，委託他人執行者，是否依個資法施行細則第8條規定，與受託者明確約定相關監督事項並為適當之監督。				
<b>九、資料安全稽核機制</b>				
(一)是否依業務規模及特性，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，並指定適當人員每年至少進行一次安維計畫及處理方法執行情形之檢查？				

稽核項目	辦理情形			發現說明
	是	否	不適用	
(二)是否將檢查結果向負責人提出報告，並由事務所負責人於紀錄確認。上開相關紀錄並應留存至少五年？				
(三)檢查結果發現安維計畫及處理方法不符法令或有不符法令之虞時，是否立即改善？				
<b>十、使用紀錄、軌跡資料及證據保存</b>				
(一)是否記錄個人資料使用情況，並留存軌跡資料或相關證據。				
(二)個人資料蒐集之特定目的消失或期限屆滿，刪除、停止處理或利用所保有之個人資料時，是否記錄個人資料之刪除、停止處理或利用之方法、時間或地點？其軌跡資料或其他相關證據及紀錄是否留存至少5年？				
(三)個人資料蒐集之特定目的消失或期限屆滿時，將停止處理或利用之個人資料移轉其他對象者，是否記錄其移轉之原因、對象、方法、時間、地點，及該對象蒐集、處理或利用之合法依據等相關證據？其軌跡資料或其他相關證據及紀錄是否留存至少5年？				
<b>十一、個人資料安全維護計畫與整體持續改善</b>				
(一)是否依事務所之規模、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)是否隨時參酌業務及本事務所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？				
(三)是否訂定業務終止後，所保有個資銷毀之方法、時間、地點及證明銷毀之方式；移轉時其移轉之原因、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；或其他刪除、停止處理或利用之方法、時間或地點；上開軌跡資料、相關證據及紀錄，應至少留存五年？				

事務所名稱：

查核人簽章：

負責人簽章：