

記帳士、記帳及報稅代理人 個人資料檔案安全維護管理措施自我檢視表

記帳士/記帳及報稅代理人姓名：

(簽名或蓋章)

事務所名稱：

執業場所地址：

聯絡電話：

E-mail：

自我檢視日期： 年 月 日

檢視項目	檢視內容	檢視結果				備註
		有/是	無/否	不適用	說明	
1. 訂定(修正)個人資料檔案安全維護計畫(本辦法第2條)	1.1 有無訂定個人資料檔案安全維護計畫(下稱本計畫)?					
	1.2 本計畫內容是否包括本辦法第3條至第21條規定相關組織及程序?					
	1.3 是否定期檢視本計畫及配合相關法令修正?					
2. 配置管理之人員及相當資源並執行任務(本辦法第3條)	2.1 就個人資料檔案安全維護管理有無指定專人或建立專責組織, 並配置相當資源?					
	2.2 專人或專責組織有無規劃、訂定、修正與執行本計畫及業務終止後個人資料處理方法等相關事項?					
	2.3 專人或專責組織有無訂定個人資料保護管理政策, 並將其所蒐集、處理或利用個人資料之依據、特定目的及其他相關保護事項, 公告使其所屬人員充分瞭解?					
	2.4 專人或專責組織有無定期對所屬人員施以基礎認知					未聘僱員工者, 本

檢視項目	檢視內容		檢視結果				備註
			有/是	無/否	不適用	說明	
		宣導或專業教育訓練，使其明瞭個人資料保護相關法令之規定、所屬人員之責任範圍及各種個人資料保護事項之方法或管理措施？					項勾選 不用。
	2.5	專人或專責組織有無定期就執行2.2至2.4任務情形向記帳士、記帳及報稅代理人或其授權人員提出書面報告？					
	2.6	本計畫之訂定或修正有無經記帳士、記帳及報稅代理人或其授權人員核定？					
3. 定期查核及界定個人資料之範圍 (本辦法第4條)	3.1	有無清查所保有之個人資料，界定其納入本計畫之範圍並建立檔案？					
	3.2	有無定期確認上述內容是否異動？					
4. 個人資料風險評估及管理機制 (本辦法第5條)	4.1	有無依據檢查項目3界定之個人資料範圍及其相關業務流程，分析可能產生風險？					
	4.2	有無依據風險分析結果，訂定適當管控措施？					
5. 事故之預防、通報及應變機制 (本辦法第6條)	5.1	有無訂定因應個人資料被竊取、竄改、毀損、滅失或洩漏等事故之適當應變措施？					
	5.2	最近1年所保有之個人資料有無發生被竊取、竄改、毀損、滅失或洩漏等事故？					無發生 事故者 本項勾 選不 適用， 並免 填 5.3 至 5.6。

檢視項目	檢視內容	檢視結果				備註	
		有/是	無/否	不適用	說明		
	5.3	發生上述事故後有無採取適當應變措施，並自發現事故時起算72小時內，檢附「個人資料侵害事故通報及紀錄表」通報財政部？					
	5.4	承5.2，有無查明事故之狀況並以適當方式通知當事人有關事實、因應措施及諮詢服務專線等？					
	5.5	承5.2，有無將事故處理情形、查處過程、結果及檢討等函報財政部？					
	5.6	發生個人資料安全事故後有無研議預防機制，避免類似事故再次發生？					
6. 依個人資料屬性分別訂定管理程序(本辦法第7條)	6.1	有無確認蒐集、處理或利用之個人資料是否包含個人資料保護法第6條所定個人資料及其特定目的？					
	6.2	有無確保蒐集、處理或利用個人資料保護法第6條所定個人資料符合相關法令之要件？					
	6.3	非個人資料保護法第6條所定個人資料，如認為具有特別管理之需要，有無訂定特別管理程序？					
7. 告知義務(本辦法第8條)	7.1	檢視蒐集、處理或利用個人資料之特定目的，除符合法定免為告知事由外，是否均依法告知當事人相關事項？					
	7.2	依資料蒐集之情況，有無採取適當之告知方式？					
8. 蒐集、處理或利	8.1	蒐集、處理個人資料是否					

檢視項目	檢視內容		檢視結果				備註
			有/是	無/否	不適用	說明	
用個人資料之特定目的及法定要件(本辦法第9條)		符合個人資料保護法第19條第1項規定，具有特定目的及法定要件？					
	8.2	利用個人資料有無符合個人資料保護法第20條第1項規定，於特定目的必要範圍內利用？					
	8.3	承上，於特定目的外利用個人資料時，有無具備法定特定目的外利用要件？					無特定目的外利用個人資料者，本項勾選不用。
9. 委託他人蒐集、處理或利用個人資料之監督(本辦法第10條)	9.1	委託他人蒐集、處理或利用個人資料之全部或一部時，有無對受託者依個人資料保護法施行細則第8條規定為適當之監督？					無委託他人蒐集、處理或利用個人資料者，9.1及9.2勾選不用。
	9.2	承上，有無明確約定相關監督事項及方式？					
10. 對於個人資料進行國際傳輸應遵循事項(本辦法第11條)	10.1	將當事人個人資料作國際傳輸者，有無檢視是否受財政部限制？					無國際傳輸者，10.1至10.3勾選不用。
	10.2	承上，有無告知當事人其個人資料所欲國際傳輸之區域？					
	10.3	承上，對資料接收方有無為本辦法第11條所列事項之監督？					
11. 因應當事人行使權利之程序(本	11.1	受理當事人就其個人資料行使個人資料保護法第3條					

檢視項目	檢視內容		檢視結果				備註
			有/是	無/否	不適用	說明	
辦法第12條)		規定權利時，有無確認其為個人資料之本人，或經個人資料之本人委託授權？					
	11.2	有無提供當事人行使權利之方式，並遵守個人資料保護法第13條有關處理期限規定？					
	11.3	如酌收必要成本費用，有無告知當事人？					
	11.4	具個人資料保護法第10條但書及第11條第2項但書、第3項但書規定得拒絕當事人行使權利之事由，有無附理由通知當事人？					
12. 維護保有個人資料正確性之措施 (本辦法第13條)	12.1	於蒐集、處理或利用過程有無檢視個人資料正確性？					
	12.2	發現個人資料不正確時，有無適時更正或補充，並通知曾提供利用之對象？					
	12.3	個人資料正確性有爭議者，有無依個人資料保護法第11條第2項規定處理？					
13. 保有個人資料特定目的消失或期限屆滿之處理程序 (本辦法第14條)	13.1	有無定期確認保有個人資料之特定目的及期限？					
	13.2	如特定目的消失或期限屆滿時，有無依個人資料保護法第11條第3項規定處理？					
14. 人員管理措施 (本辦法第15條)	14.1	有無依據作業之需要，建立管理機制，設定所屬人員不同權限，並定期確認權限內容之適當性及必要性？					未聘僱員工者，14.1至14.4勾選不適
	14.2	有無指定各相關業務流程					

檢視項目	檢視內容	檢視結果				備註
		有/是	無/否	不適用	說明	
	涉及蒐集、處理或利用個人資料之負責人員？					用。
	14.3 有無與所屬人員約定保密義務？					
	14.4 所屬人員離職時，持有之個人資料有無辦理交接，不得於離職後繼續使用，並簽署保密切結書？					
15. 資料安全管理措施(本辦法第16條)	15.1 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，有無訂定使用可攜式設備或儲存媒體規範？					
	15.2 保有之個人資料內容如有加密需要，有無於蒐集、處理或利用時，採取適當加密機制？					
	15.3 作業過程有備份個人資料需要時，有無比照原件，依個人資料保護法規定予以保護？					
	15.4 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、電腦、自動化機器設備或其他存放媒介物報廢或轉作其他用途時，有無採適當防範資料外洩措施？					
16. 以資通訊系統蒐集、處理或利用個人資料筆數達1萬筆者，應採行之資訊安全措施(本辦法第17條)	16.1 以資通訊系統蒐集、處理或利用個人資料之筆數是否達1萬筆？					本項勾選未達1萬筆者，免填16.2至16.8。
	16.2 已達1萬筆者，有無採行使					

檢視項目	檢視內容	檢視結果				備註
		有/是	無/否	不適用	說明	
	用者身分確認及保護機制？					
	16.3 承上，有無採行個人資料顯示之隱碼機制？					
	16.4 承16.2，有無採行網際網路傳輸之安全加密機制？					
	16.5 承16.2，有無採行個人資料檔案與資料庫之存取控制及保護監控措施？					
	16.6 承16.2，有無防止外部網路入侵對策？					
	16.7 承16.2，有無非法或異常使用行為之監控及因應機制？					
	16.8 承16.2，16.6及16.7部分每年有無至少辦理1次演練並檢討改善？					
17. 環境及設備安全管理措施(本辦法第18條)	17.1 保有之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、電腦或自動化機器設備等媒介物(下稱媒介物)時，針對存放儲存媒介物之環境，有無實施適當進出管制措施？					
	17.2 有無依儲存媒介物之特性及使用方式，建置適當保護設備或技術？					
	17.3 有無依所屬人員業務特性、內容及需求，訂定適當管理措施？					
18. 使用紀錄、軌跡資料及證據保存(本辦法第19條)	18.1 有無採取個人資料使用紀錄、留存自動化機器設備之軌跡資料或其他相關證據保存機制，並留存至少5年？					

檢視項目	檢視內容		檢視結果				備註
			有/是	無/否	不適用	說明	
	18.2	對於業務終止後保有之個人資料，有無採行本辦法第19條第2項規定方式處理，並留存相關紀錄、軌跡資料及相關證據至少5年？					
19. 資料安全稽核機制(本辦法第20條)	19.1	有無訂定個人資料安全稽核機制？					
	19.2	有無定期或不定期查察是否落實執行本計畫所定相關事項？					
20. 個人資料安全維護之整體持續改善機制(本辦法第21條)		有無參酌執行業務現況、社會輿情、技術發展、法令修正等因素，檢視本計畫合宜性，並適時予以修正？					

註：所稱本辦法係指「記帳士與記帳及報稅代理人個人資料檔案安全維護管理辦法」。