記帳士事務所
個人檔案安全維護計畫
及相關表格說明

社團法人臺北市記帳士公會

大綱

- 法令依據
- 事務所應處理事項
- 記帳士事務所個人資料檔案安全維護計畫參考範本
- 記帳士個人資料管理內部自主稽核表範本
- 蒐集個人資料告知事項暨個人資料提供同意書範本
- 離職員工保密切結書範本

法令依據

1. 個人資料保護法

2. 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

3. 個人資料保護法之特定目的及個人資料之類別

個人資料保護法

法令架構

章節	條文內容規範
總則	**第1條~第14條** 用詞定義、當事人權利、委外、集、處理、利用、書同意、告知義務、個資維護
公務機關對個人資料之蒐集、處理及利用	**第15條~第18條** 蒐集、處理、利用的要件、個人資料檔案公開、安全維護義務
非公務機關對個人資料之蒐集、處理及利用	**第19條~第27條** 蒐集、處理、利用的要件、國際傳輸、行政檢查、安全維護義務
損害賠償及團體訴訟	**第28條~第40條** 民事賠償責任、團體訴訟
罰則	**第41條~第50條** 刑事責任、行政處罰
附則	**第51條~第56條** 例外情形、其他規定

個人資料保護法

個人資料(第2條第1款)

姓名	出生年月日	國民身分證統一編號	護照號碼	特徵
指紋	婚姻	家庭	教育	職業
病歷	醫療	基因	性生活	健康檢查
犯罪前科	聯絡方式	財務情況	社會活動	其他得以直接或間接方式識別個人的資料

個人資料保護法

敏感個資(第6條)

概念:病歷、醫療、基因、性生活、健康檢查、犯罪前科

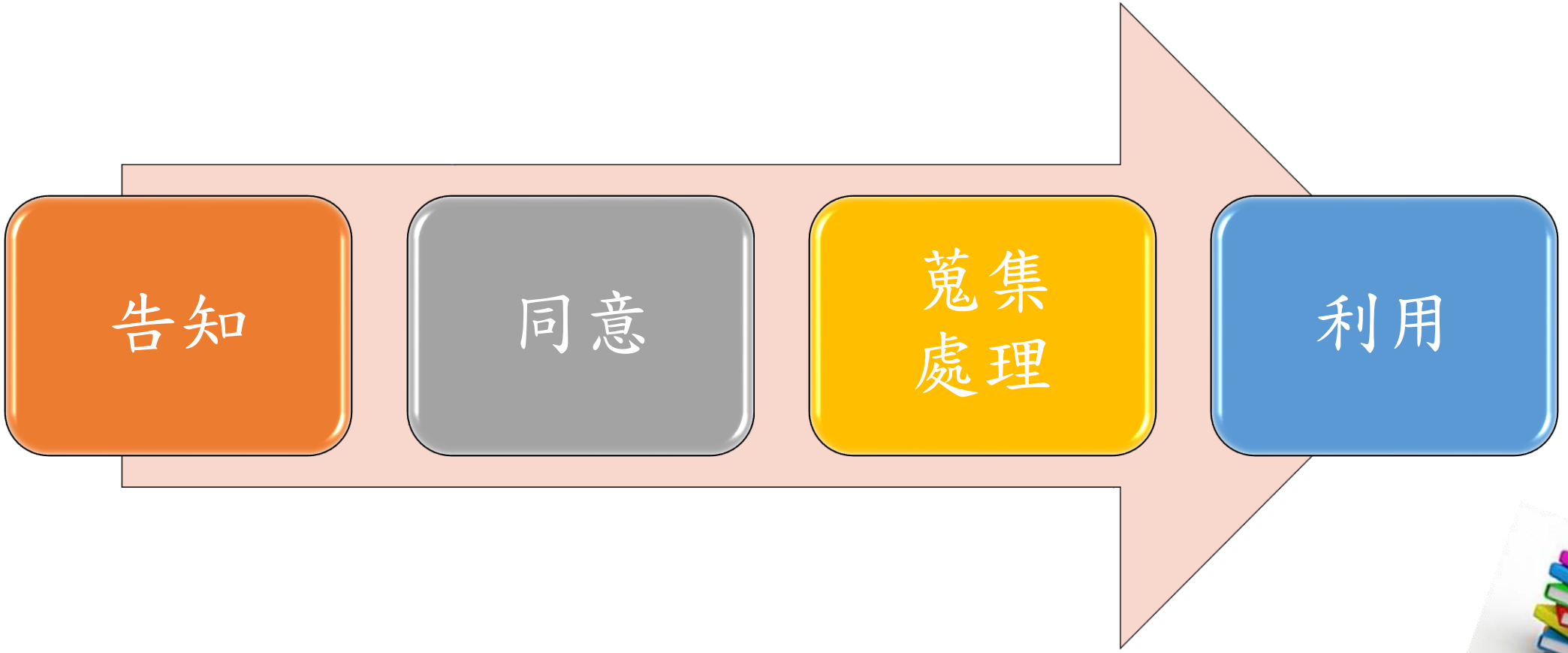
原則:不得蒐集、處理或利用

例外

- 一、法律明文規定。
- 二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
- 三、當事人自行公開或其他已合法公開之個人資料。
- 四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。
- 五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。
- 六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

個人資料保護法

資料蒐集之行為規範



個人資料保護法

告知義務(第8、9條)

直接蒐集之告知(8Ⅰ)	間接蒐集之告知(9Ⅰ)
I.公務機關或非公務機關名稱	I.公務機關或非公務機關名稱
2.蒐集之目的	2.蒐集之目的
3.個人資料之類別	3.個人資料之類別
4.個人資料利用之期間、地區對象及方式	4.個人資料利用之期間、地區對象及方式
5.當事人依第3條規定得行使之權利及方式	5.當事人依第3條規定得行使之權利及方式
6.當事人得自由選擇提供個人資料時，不提供將對其權益之影響	6.當事人得自由選擇提供個人資料時，不提供將對其權益之影響

個人資料保護法

免為告知(第8、9條)

直接蒐集之免為告知(8Ⅱ)	間接蒐集之免為告知(9Ⅱ)
1.依法律規定得免告知	I.公務機關或非公務機關名稱
2.個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要蒐集之目的	2.蒐集之目的
3.告知將妨害公務機關執行法定職務。	3.個人資料之類別
4.告知將妨害公共利益	4.個人資料利用之期間、地區對象及方式
5. 當事人明知應告知之內容	5.當事人依第3條規定得行使之權利及方式
6.個人資料之蒐集非基於營利之目的,且對當事人顯無不利之影響	6.資料來源

個人資料保護法

免為告知(第8、9條)

直接蒐集之免為告知(8Ⅱ)	間接蒐集之免為告知(9Ⅱ)
	7.當事人自行公開或其他已合法公開之個人資料
	8.不能向當事人或其法定代理人為告知
	9.基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限
	10.大眾傳播業者基於新聞報導之公益目的而蒐集個人資料

個人資料保護法

書面同意(第7條)

原始目的 (特定目的)之同意	原始目的以外目的之同意
第15條第2款及第19條項5款所稱同意，指當事人經集者告知本法所定應告知事項後，所為允許之意思表示。	第16條第7款、第20條1項第6款所稱同意。指當事人經蒐集者明告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示。

個人資料保護法

行政責任(第47條)

非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣5萬元以上50萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之

- 違反第六條第一項規定
- 違反第十九條規定
- 違反第二十條第一項規定
- 違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或處分

個人資料保護法

行政責任(第48條)

非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣2萬元以上20萬元以下罰鍰

- 違反第八條或第九條規定
- 違反第十條、第十一條、第十二條或第十三條規定
- 違反第二十條第二項或第三項規定
- 違反第二十七條第一項或未依第二項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

個人資料保護法

行政責任(第49條)

非公務機關無正當理由違反第二十二條第四項規定者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣2萬元以上20萬元以下罰鍰。

行政責任(第50條)

非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。

個人資料保護法

刑事責任(第41條)

意圖為自己或第三人不法之利益或損害他人之利益，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處5年以下有期徒刑，得併科新臺幣100萬元以下罰金。

刑事責任(第42條)

意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處5年以下有期徒刑、拘役或科或併科新臺幣100萬元以下罰金。

洗錢防制與個資法之關係

甲說：有認為洗錢防制法為特別法而個人資料保護法為普通法。

(金融監督管理委員會105.3.3金管銀法字第10400259730號函)

乙說：有認為兩者間並非特別法與普通法的關係，因此洗錢防制法在個人資料的蒐集、處理以及利用上，仍須符合個人資料保護法的例外規定。

(法務部106.1.26法律字第10603501350號函)

(國家發展委員會109.5.22日法字第|090011494號書函)

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

訂定

- 111.1.20
  訂定發布

施行

- 除第6條自發布日施行外，
  其餘自111.7.20施行

建立內部控制及稽核規範

第2條

- 訂定安全維護計畫

第3條

- 專人(專責組織)管理

第20條

- 定期或不定期稽核

蒐集、處理或利用之應注意事項

蒐集、處理或利用個資

§8	告知當事人
§9	目的範圍內為之且符合法定要件
§9	目的外使用應符合法定要件
§13	維護個人資料正確性
§14	目的消失或期限屆滿應停止利用

應採行個資管理措施(1/6)

人員管理措施(§15)

建立管理機制，
設定所屬人員
不同權限

指定個人資料
之負責人員

與所屬人員
約定保密義務

所屬人員離職後
不得繼續使用，
並簽署保密切結書

應採行個資管理措施(2/6)

資料安全管理措施(§16)

訂定使用可攜式設備或儲存媒體規範

採取適當加密機制

備份資料應比照原件同等保護

儲存媒介物報廢或轉作其他用途，應採取適當防範資料外洩措施

應採行個資管理措施(3/6)

巨量個資強化資訊安全措施(§17)

適用對象	個資筆數達一萬筆者
採行措施	➢ 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
	➢ 檔案與資料庫之存取控制及保護監控措施
	➢ 防止外部網路入侵對策
	➢ 非法或異常使用行為之監控及因應機制

定期演練
檢討改善

應採行個資管理措施(4/6)

環境及設備安全管理措施(§18)

存放媒介物之環境，實施進出管制措施

建置適當保護設備或技術

依業務特性訂定適當管理措施

應採行個資管理措施(5/6)

留存紀錄(§19)

保存範圍

- 使用個資紀錄、機器設備軌跡資料或其他相關證據
- 留存銷毀、移轉、刪除、停止處理或利用個人資料相關紀錄

保存期間

- 至少五年

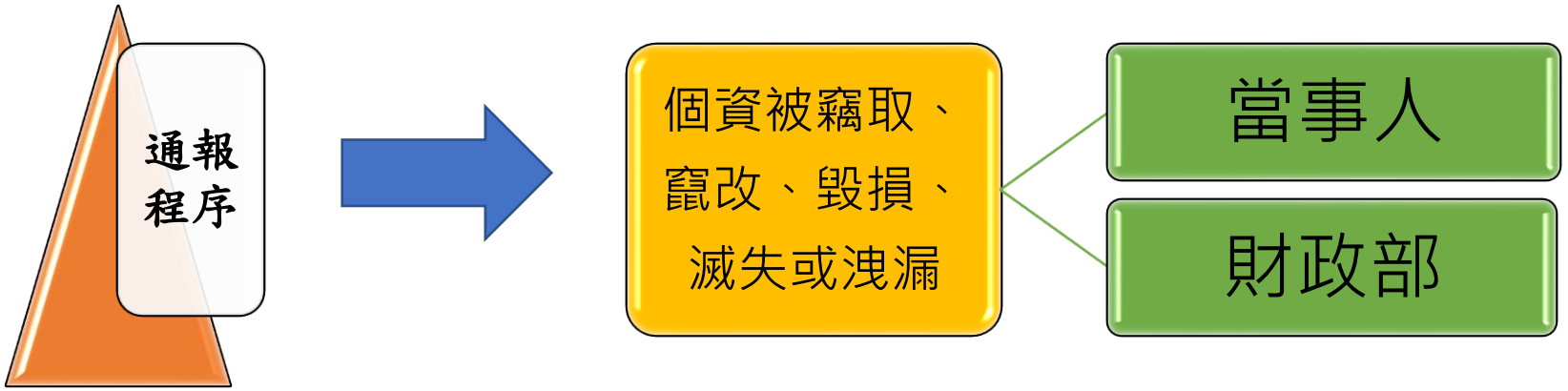
應採行個資管理措施(6/6)

事故預防、通報及應變措施(§6)

適當應變措施，控制損害

查明事故並通知當事人

研議預防機制



事務所應該做甚麼?

事務所計畫

- 擬定事務所個人資料檔案安全維護計畫
- 定期對所屬人員施以基礎認知宣導或專業教育訓練
- 訂定「記帳士個人資料管理內部自主稽核表」
- 定期或不定期稽核

應備文件

- 蒐集個人資料告知事項暨個人資料提供同意書
- 離職員工保密切結書

記帳士事務所個人資料檔案安全維護計畫範本介紹(1/18)

壹、記帳士事務所之組織及規模

貳、個人資料檔案安全維護管理措施

一、依據

二、個人資料檔案安全維護計畫之訂定及修正

三、專責人員及資源配置

四、本事務所之告知義務及當事人可行使的權利

五、本事務所保有個人資料情形

六、風險分析及管理機制

七、預防個人資料事故及通報措施

八、本事務所蒐集、處理、利用及維護個人資料情形

九、本事務所之個人資料管理措施

十、安全稽核機制

十一、個人資料使用紀錄、軌跡資料及證據保存機制

十二、附表：個人資料侵害事故通報及紀錄表

記帳士事務所個人資料檔案安全維護計畫範本介紹(2/18)

○○○記帳士事務所個人資料檔案安全維護計畫

（參考範本）

**本範本僅供參考，請依事務所內部管理作業程序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等相關事項。

訂定日期：中華民國111年00月00日

記帳士事務所個人資料檔案安全維護計畫範本介紹(3/18)

壹、記帳士事務所之組織及規模

一、組織型態：獨資或合夥

二、事務所地址：○○○

三、負責人：○○○

四、人數：負責人以外之記帳士：○人(聯合事務所適用)

員工：○人（可記載一定範圍之正職員工）

記帳士事務所個人資料檔案安全維護計畫範本介紹(4/18)

貳、個人資料檔案安全維護管理措施

一、依據：

個人資料保護法第27條第3項及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第2條規定辦理。

二、個人資料檔案安全維護計畫之訂定及修正

(一)訂定目的：為防止個人資料被竊取、竄改、毀損、滅失或洩漏，爰訂定「個人資料檔案安全維護計畫」（下稱本計畫），本事務所員工應依本計畫辦理個人資料檔案安全管理及維護事宜。

(二)本計畫將參酌執行業務現況、社會輿情、技術發展、法令修正等因素，檢視其合宜性，並經負責人或其授權人員於核定後予以修正。

記帳士事務所個人資料檔案安全維護計畫範本介紹(5/18)

三、專責人員及資源配置

(一)專責人員：

1.姓名：○○○。（得配置專責人員或由記帳士本人執行）

2.職責：

(1)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)訂定個人資料保護管理政策，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，公告使本事務所員工充分瞭解。

(3)定期對本事務所員工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之規定、責任範圍及各種個人資料保護事項之方法或管理措施。

(4)定期(每年至少1次)就執行前開任務情形向負責人或其授權人員提出書面報告。

(二)預算：每年新臺幣○○○元。（包含管理薪資、設備費用等，可記載一定範圍之金額，依實際狀況填寫）

(三)個人資料保護管理政策：遵循個人資料保護法關於蒐集、處理及利用個人資料之規定，並確實維護與管理所保有個人資料檔案安全，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。

記帳士事務所個人資料檔案安全維護計畫範本介紹(6/18)

四、本事務所之告知義務及當事人可行使的權利

(一)本事務所之告知義務

1.本事務所直接向當事人蒐集個人資料時，應明確告知以下事項：

(1)事務所名稱。

(2)蒐集目的。

(3)個人資料之類別。

(4)個人資料利用之期間、地區、對象及方式。

(5)當事人得請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料。

(6)當事人得自由選擇提供個人資料，及不提供將對其權益之影響。

記帳士事務所個人資料檔案安全維護計畫範本介紹(7/18)

2.本事務所之告知方式，包括言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉等方式。

3.本事務所蒐集非由當事人提供之個人資料，應於處理或利用前向當事人告知個人資料來源及前項應告知之事項，若當事人表示拒絕，應立即停止處理、利用其個人資料。

4.本事務所與當事人簽訂之委託書，如獲得當事人書面同意，得進行個人資料蒐集、處理及利用，並於委託期限屆滿時主動刪除或銷毀。但因法令規定或執行業務所必須或經客戶書面同意者，不在此限。

（二)當事人可行使的權利

1.應依當事人之請求，就其個人資料得查詢或請求閱覽、製給複製本、補充、更正、停止蒐集、處理或利用或請求刪除，本事務所不得請其預先拋棄或以特約限制之。

2.當事人就其個人資料行使權利事項如有個人資料保護法第10條但書、第11條第2項但書及第3項但書規定得拒絕當事人行使權利之事由，本事務所應附理由通知當事人。

3.本事務所處理本項業務時，應確認其為個人資料之本人，或經個人資料之本人委託授權。本項業務之連絡窗口為：○○○；電話：○○○○○○，並將聯絡窗口及電話等資料，揭示於本事務所營業處所佈告欄或網頁。

記帳士事務所個人資料檔案安全維護計畫範本介紹(8/18)

五、本事務所保有個人資料之類別、範圍與目的

（一）特定目的：會計與相關服務(129)、人事管理(002)。

（視各事務所業務情形自行清查後填具資料）

（二）資料類別：

辨識個人者：如客戶及員工之姓名、出生年月日、身分證統一編號、婚姻、家庭、職業、健康檢查、財產狀況、聯絡方式等，及其他得以直接或間接識別該個人之資料。

六、風險分析及管理機制

(一)風險評估

1. 經由本事務所電腦下載或外部網路入侵而外洩。
2. 經由接觸書面契約而外洩。
3. 員工及第三人故意竊取、竄改、毀損、滅失或洩漏。

(二)管理機制

1. 每位員工均應以其使用者代碼及密碼登入事務所電腦，並定期進行網路資訊安全維護及控管。
2. 列冊管理書面契約，落實員工查(調)閱書面契約紀錄管理。
3. 加強員工管理及事務所出入人員管制。

記帳士事務所個人資料檔案安全維護計畫範本介紹(9/18)

七、預防個人資料事故及通報措施

(一)預防措施

1. 本事務所員工如因其工作執掌而須使用事務所電腦輸出、輸入個人資料時，均須鍵入其使用者代碼及密碼，同時在使用範圍及使用權限內為之。

2. 非主辦業務之員工查閱契約書類時，應經負責人或其授權人員之同意。

3. 加強管控本事務所員工對內或對外之個人資料傳輸，避免外洩。

4. 加強員工之個人資料保護相關法規教育訓練。

(1)每年至少進行◯次個人資料保護相關法規教育訓練及宣導，使本事務所人員知悉應遵守之規定，並留存相關紀錄（例如：簽名冊等文件）。

(2)對於新進人員應特別給予指導，使其明瞭個人資料保護相關法規、責任範圍及應遵守之管理措施。

記帳士事務所個人資料檔案安全維護計畫範本介紹(10/18)

(二)應變措施

1.發現本事務所有個人資料遭竊取、竄改、毀損、滅失或洩漏之情形，應立即通報負責人並查明發生原因及責任歸屬，及依實際狀況採取相關應變措施，以控制事故對當事人之損害。

2.對於個人資料遭竊取、竄改、毀損、滅失或洩漏之當事人，應以適當方式通知當事人，使其知悉及本事務所持有個人資料發生事故、已採取之處理措施、諮詢服務電話及聯絡窗口等資訊。

3.針對事故發生原因研議預防機制，避免類似事故再次發生。

(三)通報措施

本事務所應自發現事故時起算72小時內，填具「個人資料侵害事故通報及紀錄表」，以電子郵件方式向財政部通報，並將視案情發展適時通報處理情形，以及將整體查處過程、結果及檢討等函報財政部。

記帳士事務所個人資料檔案安全維護計畫範本介紹(11/18)

八、本事務所蒐集、處理、利用及維護個人資料情形

(一)本事務員工因執行業務而蒐集、處理個人資料時，應檢視是否符合個人資料保護法第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；為特定目的外之利用時，應檢視是否符合個人資料保護法第20條第1項但書情形。

(二)本事務所依個人資料屬性，分別訂定下列管理程序：

1.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。

2.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。

(三)維護個人資料正確性之方式

1.於蒐集、處理或利用過程檢視個人資料正確性。

2.發現個人資料不正確時，適時更正或補充，並通知曾提供利用之對象。

3.個人資料正確性有爭議者，主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議者，不在此限。

記帳士事務所個人資料檔案安全維護計畫範本介紹(12/18)

(四)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。

1.定期確認保有個人資料之特定目的及期限，如特定目的消失或期限屆滿時，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。

2.對於業務終止後保有之個人資料，依下列方式處理，相關紀錄應保存5年：

(1)銷毀：銷毀之方法、時間、地點及證明銷毀方式。

(2)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。

(3)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。

(五)本事務所如委託他人蒐集、處理或利用個人資料之全部或一部時，對受託者應為適當之監督，並明確約定相關監督事項及方式。

(六)本事務所將當事人個人資料作國際傳輸者，應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。

記帳士事務所個人資料檔案安全維護計畫範本介紹(13/18)

九、本事務所之個人資料管理措施

(一)人員管理措施

1.本事務所依員工（例如主管、非主管人員）之業務需求設定不同之個人資料使用權限，並定期(每年至少1次)確認權限內容之適當性及必要性。

2.本事務所員工使用電腦設備蒐集、處理、利用個人資料，應以專屬帳號密碼登入電腦系統，其帳號密碼應保密，不得洩漏或與他人共用，密碼應每○天（週、月、年）變更，並於變更密碼後始可繼續使用電腦；如因業務需要須利用非權限範圍之個人資料時，應事前提出申請，經業務主管人員同意後開放權限利用。

3.本事務所依業務流程指定個人資料蒐集、處理或利用之負責人員，相關負責個人資料檔案管理人員於職務異動時，應移交其保管之檔案資料，接辦人員應另行設定密碼。

4.本事務所人員應妥善保管個人資料之儲存媒介物，執行業務時應依個人資料保護法規定蒐集、處理及利用個人資料。

5.本事務所與員工之勞務契約應納入「員工於任職期間因業務所接觸個人資料均負保密義務」之相關保密條款。員工離職時，持有之個人資料應辦理交接，不得於離職後繼續使用，並簽署保密切結書。

記帳士事務所個人資料檔案安全維護計畫範本介紹(14/18)

(二)環境、設備及資料安全管理措施

1. 書面資料檔案管理

(1)以書面資料儲存個人資料者，應設置專屬儲存空間並列冊管理。

(2)書面資料儲存空間應指派專人管理，並將調閱或使用個人資料情形作成書面紀錄，且事務所員工非經負責人或其授權人員同意不得任意複製或影印資料。

(3)書面資料儲存空間應設置防火設備或其他相關防護措施設備，以防止資料滅失或遭竊取。

(4)以書面儲存之個人資料，於銷毀前應以碎紙設備進行處理。

記帳士事務所個人資料檔案安全維護計畫範本介紹(15/18)

2.運用電腦及儲存媒介儲存個人資料管理

(1)指派專人管理用於儲存個人資料之電腦，本事務所員工應以其專屬帳號密碼登入始得使用電腦，並留存使用紀錄；該電腦不得作為公眾查詢之前端工具。

(2)用於儲存個人資料之電腦，應安裝防毒軟體、定期掃毒，並定期進行電腦保養維護，於保養維護或更新設備時，應注意資料之備份及相關安全措施。

(3)指派專人管理用於儲存個人資料之儲存媒介，儲存媒介使用完畢應即退出，不得任意放置在電腦，並就其使用情形作成書面紀錄。

(4)用於儲存個人資料之儲存媒介非經負責人或其授權人員同意並作成紀錄不得攜帶外出或拷貝複製。

(5)運用電腦及儲存媒介儲存之個人資料應定期(例如：每月)備份，並比照原件予以保護。

(6)儲存個人資料之電腦及儲存媒介於報廢、汰換或轉作其他用途前，應由本事務所負責人或其授權人員檢視各該設備儲存之個人資料是否確實刪除。

(7)重要個人資料應另加設管控密碼，非經陳報負責人或經指定之管理人員核可，並取得密碼者，不得存取。

(8)於放置電腦及儲存媒介之空間設置防火及其他相關防護措施設備，以防止資料滅失或遭竊取。

記帳士事務所個人資料檔案安全維護計畫範本介紹(16/18)

3.本事務所使用資通訊系統蒐集、處理或利用消費者個人資料達一萬筆以上時，應於保有筆數達一萬筆之日起算6個月內採取下列資訊安全措施：

(1)使用者身分確認及保護機制。

(2)個人資料顯示之隱碼機制。

(3)網際網路傳輸之安全加密機制。

(4)個人資料檔案與資料庫之存取控制及保護監控措施。

(5)防止外部網路入侵對策。

(6)非法或異常使用行為之監控及因應機制。

4.前開(1)至(5)所定措施，每年至少辦理一次演練並檢討改善。

記帳士事務所個人資料檔案安全維護計畫範本介紹(17/18)

十、安全稽核機制

(一)本事務所定期(每年至少1次)辦理個人資料檔案安全維護稽核，檢查本事務所是否落實本計畫規範事項，針對檢查結果不符合及潛在風險事項規劃改善措施，確保相關措施之執行。執行改善與預防措施時，應依下項事項辦理：

1. 確認不符合事項之內容及發生原因。
2. 提出改善及預防措施方案。
3. 紀錄檢查情形及結果。

(二)前項檢查情形及結果應載入稽核報告中，由事務所負責人簽名確認。

十一、個人資料使用紀錄、軌跡資料及證據保存機制

本事務所應採行適當資料安全維護措施，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至少五年等機制，以供必要時說明其所定本計畫執行情況。

十二、附表：個人資料侵害事故通報及紀錄表

記帳士事務所個人資料檔案安全維護計畫範本介紹(18/18)

事故通報及紀錄單

個人資料侵害事故通報及紀錄表		
記帳士事務所： 姓名：	通報時間： 年 月 日 時 分 通報人： （簽章） 職稱： 電話： 電子郵件： 地址：	
事件發生時間		
事件發生種類	竊取 洩漏 竄改 毀損 滅失 其他侵害事故	個資侵害之總比數 （大約） 筆 ☐ 一般個資 筆 ☐ 特種個資 筆
發生原因及事件摘要		
損害狀況		
個資侵害可能結果		
擬採取之因應措施		
擬採通知當事人之時間及方式		
是否於發現個資外洩後72小時內通報		☐是 ☐否，理由

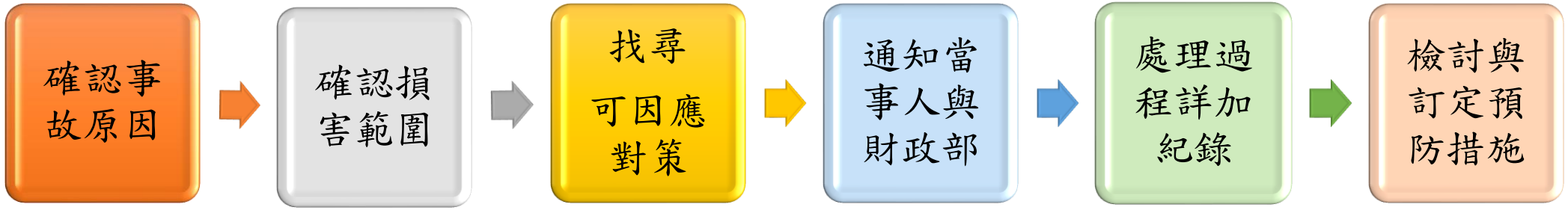
財政部(賦稅署)通報聯繫窗口

電子郵件：dot_ycchen@mail.mof.gov.tw

聯絡電話：(02)23228000分機8199

記帳士事務所個人資料檔案安全維護計畫

- 事故處理流程



記帳士個人資料管理內部自主稽核表

- 一、專責人員及資源
- 二、個人資料之範圍界定
- 三、風險分析及管理機制
- 四、預防個人資料事故及通報措施
- 五、個人資料蒐集、處理及利用之內部管理程序
- 六、個人資料管理措施
- 七、人員管理措施
- **八、設備安全管理**
- **九、資料安全稽核機制**
- **十、使用紀錄、軌跡資料及證據保存**

記帳士個人資料管理內部自主稽核表

內容說明(1/4)

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	
一、專責人員及資源				
(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？				
二、個人資料之範圍界定				
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？				
三、風險分析及管理機制				
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？				
四、預防個人資料事故及通報措施				
(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？				
五、個人資料蒐集、處理及利用之內部管理程序				
(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；為特定目的外之利用時，應檢視是否符合本法第20條第1項但書				

記帳士個人資料管理內部自主稽核表

內容說明(2/4)

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	
(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。				
六、個人資料管理措施				
(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？				
(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？				

記帳士個人資料管理內部自主稽核表

內容說明(3/4)

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	
七、人員管理措施				
(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？				
八、設備安全管理				
(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。				
九、資料安全稽核機制				
(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？				
(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？				

記帳士個人資料管理內部自主稽核表

內容說明(4/4)

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	
十、使用紀錄、軌跡資料及證據保存				
(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？				
十一、個人資料安全維護計畫與整體持續改善				
(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：

蒐集個人資料告知事項暨個人資料提供同意書範本(1/2)

蒐集個人資料告知事項暨個人資料提供同意書(參考範本)

蒐集個人資料告知事項（註:亦可將告知事項暨同意書內容加註於客戶委託書內）

本事務所遵守個人資料保護法規定,在您提供個人資料予本所前,依法告知下列事項:)

一、000記帳士事務所(以下簡稱本所)因協助設立、帳務等目的而獲取您下列個人資料類別:姓名、出生年月日、國民身分證統一編號、性別、職業教育 、連絡方式(包括但不限於電話號碼、E-MAIL、居住或工作地址)等或其他得以直接或間接識別您個人之資料。

二、本所將依個人資料保護法及相關法令之規定下,依本所個人資料檔案安全維護計畫,蒐集、處理及利用您的個人資料。

三、本所將於蒐集目的之存續期間合理利用您的個人資料。

四、除蒐集之目的涉及國際業務或活動外,本所僅於中華民國領域內利用您的個人資料。

五、您可依個人資料保護法第3條規定,就您的個人資料向本所行使之下列權利:

(一)查詢或請求閱覽。

(二)請求製給複製本。

(三)請求補充或更正。

蒐集個人資料告知事項暨個人資料提供同意書範本(2/2)

(四)請求停止蒐集、處理及利用。

(五)請求刪除。

六、您因行使上述權利而導致對您的權益產生減損時,本所不負相關賠償責任。

七、另依個人資料保護法第14條規定,本所得酌收行政作業費用。

八、若您未提供正確之個人資料,本所將無法為您提供特定目的之相關業務。

九、本所因業務需要而委託其他機關處理您的個人資料時,本所將會善盡監督之責。

十、您瞭解此一同意書符合個人資料保護法及相關法規之要求,且同意本所留存此同意書,供日後取出查驗。

個人資料之同意提供

一、本人已充分知悉貴所上述告知事項。

二、本人同意貴所蒐集、處理、利用本人之個人資料,以及其他公務機關請求行政協助目的之提供。

立同意書人: (簽章)

中華民國 年 月 日

離職員工保密切結書(範本)(1/2)

(註：可將此表內容併入事務所員工到職合約內，不另簽署)

本人茲聲明並保證：

一、本人於任職000記帳士事務所期間，於職務上所知悉或使用之000記帳士事務所之營業秘密，依營業秘密法第三條規定，均屬000記帳士事務所所有，本人離職後即無權繼續持有、使用上開營業秘密，亦不得直接或間接使任何第三人持有、使用之(不論本人或該第三人是否出於營利目的)。

二、本人於000記帳士事務所任職期間，於職務上，依個人資料保護法而蒐集、處理或知悉之他人個人資料，本人離職後即無權繼續持有、使用，亦不得直接或間接使任何第三人持有、使用之(不論本人或該第三人是否出於營利目的)。

離職員工保密切結書(範本)(2/2)

三、本人任職期間持有之000記帳士事務所全部報告書、報價單、比價表、廠商報價單、契約書及其他法律文件、函文、簽呈、人事資料、財務資料等任何與000記帳士事務所業務及運營有關之資料，不論其以紙本、電子檔案、即時通訊軟體通訊紀錄、e-mail 或其他任何有形或無形方式承載，亦不論為正本、副本、抄本或影本，均已完整交還予000記帳士事務所收執，本人絕無保留、保存、抄錄或複製前開資料，亦不會於離職後以他法使第三人知悉前開資料之部分或全部內容。

四、除法令另有規定外，以上保密切結於本人離職後三年內有效。

五、如本人違反前開聲明與保證事項，願依營業秘密法、個人資料保護法及其他相關法令負相關之刑事及民事責任，如致生損害於000記帳士事務所者，願負損害賠償責任，絕不異議。

立切結書人:　(簽章)

身分證字號:

中華民國　年　月　日

報告完畢
謝謝聆聽