中華民國地政士公會全國聯合會　函

會址：台北市中山區建國北路一段156號9樓
電話：(02) 2507-2155
傳真：(02) 2507-3369
電子信箱：angela.echo@msa.hinet.net
網　　址：www.rocrea.org.tw
聯絡人：蘇麗環(分機：15)

110、12、9 基字收文第 425 號

受文者：本會所屬各會員公會

發文日期：中華民國 110 年 12 月 09 日
發文字號：全地公(9)字第 1109864 號
速別：
密等及解密條件：
附件：

主　旨：檢送有關第 1 次修正後之「內政部指定地政類非公務機關個人資料檔案安全維護管理辦法」-地政士事務所個人檔案安全維護計畫等範本草案(修正版)，再次供請 貴會參考，並請續協助依本業業別特性，檢視該範本草案內容是否妥適，轉請 查照。

說　明：

一、鑑於「內政部指定地政類非公務機關個人資料檔案安全維護管理辦法」業於 110 年 11 月 30 日發布在案，有關該辦法第四條規定各事務所應訂定「地政士事務所個人檔案安全維護計畫及業務終止後個人資料處理方法」1 節，內政部已草擬範本(詳如後附件 1：第 1 次修正後版本)，以供請 參考。

二、茲請 貴會續協助依地政士之行業別特性，檢視該範本草案內容是否妥適或有不完善之處，均惠請於本(12)月 24 日前回覆本會，俾供彙整意見後送請內政部修正調整。

三、隨函另提供有關「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者應採取之資訊安全措施相關說明」1份(附件2)，請 查收。

正　本：本會所屬各會員公會

理事長 李嘉嬴

○○○地政士事務所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

壹、地政士事務所之組織及規模

一、組織型態（事務所或聯合事務所）：

二、事務所地址：

三、負責人：○○○

四、人數：負責人以外之地政士：○人

員工：○人（可記載一定範圍之人數）

貳、個人資料檔案之安全維護管理措施（計畫內容）

一、管理人員及資源

（一）管理人員：

1、配置人數：○人。（至少配置1名管理人員）

2、職責：負責規劃、訂定、修正與執行計畫或業務終止後個人資料處理方法等相關事項，並向負責人提出報告。

（二）預算：每一年新台幣○○萬元。（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、篡改、毀損、滅失或洩漏。

二、個人資料之範圍

（一）特定目的：

不動產服務、代理與仲介業務、契約或類似契約或其他法律關係事務、消費者客戶管理與服務、人事管理。（類別：識別類）

（二）客戶個人資料：

本計畫所稱之客戶個人資料，除係指客戶姓名、出生年月日、國民身分證統一編號、婚姻、家庭、教育、職業、聯絡方式外及其他得以直接或間接方式識別該個人之資料。

（三）員工或所屬地政士個人資料：

指姓名、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。

三、風險評估及管理機制

（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、經由接觸書面契約書類而外洩。

3、員工故意竊取、毀損或洩漏。

（二）管理機制

1、藉由使用者代碼、識別密碼設定及文件妥適保管。

2、定期進行網路資訊安全維護及控管。

3、加強對員工之管制及設備之強化管理。

四、事故之預防、通報及應變機制

（一）預防：

1、本事務所員工或所屬之地政士如因其工作執掌而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之。

2、非承辦之地政士或員工參閱契約書類時，應得事務所負責人或經指定之管理人員之同意。

3、加強員工教育宣導，並嚴加管制。

（二）通報及應變：

1、發現個人資料遭竊取、竄改、毀損、滅失或洩漏即向事務所負責人通報，並立即查明發生原因及責任歸屬，及依實際狀況採取必要措施。

2、對於個人資料遭竊取之客戶，以書面通知使其知悉及本事務所已採取之處理措施及諮詢服務專線。

3、針對事故發生原因研議改進措施。

4、遇有達1,000筆以上之個人資料事故時，應於發現後72小時內，以書面通報○○市（縣）政府地政局，並副知內政部。（書面通報格式詳如內政部指定地政類非公務機關個人資料檔案安全維護管理辦法第8條規定）

五、個人資料蒐集、處理及利用之內部管理措施

（一）直接向當事人蒐集個人資料時，應明確告知以下事項：a. 事務所名稱。b. 蒐集目的。c. 個人資料之類別。d. 個人資料利用之期間、地區、對象及方式。e. 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。

（二）所蒐集非由當事人（或客戶）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。

（三）與客戶簽訂之委託書，如獲得客戶書面同意，得進行個人資料蒐集、處理及利用。於委託期限屆滿時應主動刪除或銷毀。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。

（四）客戶表示拒絕行銷或請求閱覽、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時，連絡窗口為：○○○ ；電話為：○○○○○○。並將聯絡窗口及電話等資料，揭示於本事務所營業處所或網頁。如認有拒絕當事人行使上述權利之事由，應附理由通知當事人。

（五）負責保管及處理個人資料檔案之人員，其職務有異動時， 應將所保管之儲存媒體及有關資料檔案移交，以利管理

（六）本事務所員工或所屬之地政士如因其工作執掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。

（七）由指定之管理人員定期清查所保有之個人資料是否符合蒐集特定目的，若有非屬特定目的必要範圍之資料，或特定目的消失、期限屆滿而無保存必要者，即予刪除、銷毀或其他適當處置。

（八）本事務所如有委託他人（或他公司）蒐集、處理或利用個人資料時，當對受託者為適當之監督並與其明確約定相關監督事項。

（如未委託他人則可以選擇加以刪除）

（九）所蒐集之個人資料如需作特定目的外利用，必須先行檢視是否符合規定。

（十）本事務所因故終止業務時，原保有之個人資料，即依規定不再使用，

並採銷毀、移轉或其他妥適方式處理。

六、設備安全管理、資料安全管理及人員管理措施

（一）設備安全管理

1、建置個人資料之有關電腦設備，資料保有單位應定期保養維護，於保養維護或更新設備時，並應注意資料之備份及相關安全措施。

2、建置個人資料之個人電腦，不得直接作為公眾查詢之前端工具。

3、事務所應指派專人管理儲存個人資料之相關電磁紀錄物或相關媒體資料，非經負責人同意並作成紀錄不得攜帶外出或拷貝複製。

4、本事務所之客戶個人資料檔案應定期（例如：每二週）下載以作為備份。

5、重要個人資料備份應異地存放，並應置有防火設備及保險箱等防護設備，以防止資料滅失或遭竊取。

6、電腦、自動化機器或其他存放媒介物需報廢汰換或轉作其他用途時，本事務所負責人或經指定之管理人員應檢視該設備所儲存之個人資料是否確實刪除。

（二）資料安全管理

1、電腦存取個人資料之管控：

（1）個人資料檔案儲存在電腦硬式磁碟機上者，應在個人電腦設置識別密碼、保護程式密碼及相關安全措施。

（2）本事務所員工或所屬地政士如因其工作執掌相關而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之，其中識別密碼並應保密，不得洩漏或與他人共用。

（3）個人資料檔案使用完畢應即退出，不得任其停留於電腦終端機上。

（4）定期進行電腦系統防毒、掃毒之必要措施。

（5）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。

2、紙本資料之保管：

（1）對於各類委託書、契約書件（含個人資料表）應存放於公文櫃

內並上鎖，員工或所屬地政士非經事務所負責人或經指定之管理人員同意不得任意複製或影印。

（2）對於記載個人資料之紙本丟棄時，應先以碎紙設備進行處理。

3、因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10,000筆以上，爰針對該資通訊系統，採取下列資訊安全措施：（註：如事務所未有此情況，本項敘述可以刪除）

（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。

（三）人員安全管理

1、本事務所依業務需求，得適度設定所屬人員（例如主管、非主管人員）不同之權限，以控管其個人資料之情形。

2、本事務所員工或所屬之地政士每○天（週、月）應變更識別密碼1次，並於變更識別密碼後始可繼續使用電腦。

3、員工離職或所屬之地政士與事務所終止僱傭或合夥契約時，將立即取消其使用者代碼（帳號）及識別密碼。其所持有之個人資料應辦理交接，不得在外繼續使用，並簽訂保密切結書（如在任職時之相關勞務契約已有所約定時，亦屬之）。

4、本事務所員工及所屬地政士應妥善保管個人資料之儲存媒介物，執行業務時依個人資料保護法規定蒐集、處理及利用個人資料。

5、本事務所與員工或所屬之地政士所簽訂之相關勞務契約或承攬契約均列入保密條款及相關之違約罰則，以確保其遵守對於個人資料內容之保密義務（含契約終止後）。

七、認知宣導及教育訓練

（一）本事務所每年進行個人資料保護法基礎教育宣導及教育訓練至少○次，使員工或所屬之地政士知悉應遵守之規定。前述教育宣導及訓練應留存紀錄（例如：簽名冊等文件）

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

八、個人資料安全維護稽核機制

（一）本事務所定期（每半年至少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事項及潛在不符合之風險，應規劃改善措施，並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。

九、使用記錄、軌跡資料及證據保存

（一）本事務所建置個人資料之電腦，其個人資料使用查詢紀錄檔，每年定期備份加密，並將該紀錄檔之儲存媒介物保存於適當處所以供檢查。

（二）個人資料使用紀錄以紙本登記者，應存放於公文櫃內並上鎖，非經本事務所負責人或經指定之管理人員同意，不得任意取出。

（註：本項請依實際情形說明事務所如何保存，例如：個人資料使用查詢紀錄、自動化機器設備之軌跡資料。）

十、個人資料安全維護之整體持續改善

（一）本事務所將隨時依據計畫執行狀況，注意相關技術發展及法令修正等事項，檢討本計畫是否合宜，並予必要之修正。

（二）針對個資安全稽核結果不符合法令之虞者，規劃改善與預防措施。

十一、業務終止後之個人資料處理方法

本事務所業務終止後，所保有之個人資料不得繼續使用，並依實際情形採下列方式處理，並留存相關紀錄：

（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。

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者應採取之資訊安全措施相關說明

一、依據內政部指定地政類非公務機關個人資料檔案安全維護管理辦法第16條規定：「非公務機關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者，應採取下列資訊安全措施：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。前項第五款及第六款所定措施，應定期演練及檢討改善。」

二、如事務所有符合上述之情形者，針對該資通訊系統，應至少有上述六項資訊安全措施。為利實作，以下提供針對六項資訊安全措施之說明，請提供事務所之資訊人員，或事務所資通訊系統之建置廠商，供其參考，俾利建置相關資安措施。

＊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，針對六項資訊安全措施之實作說明如下：

項目	資訊安全措施	實作說明
一	使用者身分確認及保護機制	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	個人資料顯示之隱碼機制	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 29191「資訊技術－安全技術－部分匿名及部分去連結鑑別之要求事項」國家標準。
三	網際網路傳輸之安全加密機制	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。
四	個人資料檔案與資料庫	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

	之存取控制及保護監控措施	識別、鑑別及身分管理，並採用最小權限原則進行存取控制管理。
五	防止外部網路入侵對策	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。
六	非法或異常使用行為之監控及因應機制	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。