

內政部 函

地址：408205臺中市南屯區黎明路2段503號

聯絡人：廖淑韻

聯絡電話：04-22502228

傳真：04-22502372

電子信箱：moi3264@land.moi.gov.tw

受文者：新竹市政府

發文日期：中華民國111年1月14日

發文字號：台內地字第1100267068號

速別：普通件

密等及解密條件或保密期限：

附件：如文(請至本部附件下載區 <https://DOC3DL.moi.gov.tw/DL/DL1/DLI100.aspx> 以發文字號及發文日期下載，有效下載期限1個月。) 識別碼：Z0AAMSAW。

主旨：檢送不動產經紀業個人資料管理內部自主稽核表及其法規依據、相關說明等各1份，請轉所屬會員參考運用並確實依相關規定辦理，請查照。

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18條及第23條等規定辦理。
- 二、為避免人格權受侵害，並促進個人資料之合理利用，本部依據個人資料保護法第27條第3項規定於110年11月30日訂定上開辦法，依辦法第23條規定，不動產經紀業應於發布施行日起6個月內(即111年6月1日以前)，依該辦法規定修正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。另為確保上開安維計畫及處理方法之落實，同辦法第18條第1項及第2項規定，應依其業務規模及特性，衡酌經營資源之合理分配，訂定個人資

地政處

111/01/14 15:18



1110019292

無附件

料安全維護稽核機制，並指定適當人員每半年至少進行1次安維計畫及處理方法執行情形之檢查，檢查結果應向負責人提出報告，並留存相關紀錄至少5年。先予敘明。

三、又不動產經紀業個人資料檔案安全維護計畫範本前經貴會於102年訂定並提供所屬會員參考，茲為促進貴會會員落實上開辦法規定，請儘速配合修正該計畫範本內容，並請提醒所屬會員應視其業務規模、特性、保有個人資料之性質、數量及相關規定等事項，自行酌修。另為協助落實安維計畫及處理方法之稽核機制，爰提供內部自主稽核表及其法規依據及相關說明等（含「不動產經紀業個人資料管理內部自主稽核表」、「不動產經紀業個人資料管理內部自主稽核檢核表法規依據及說明」及「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」等3種）供參，貴會會員應確實依相關規定辦理稽核，並留存相關紀錄，以供必要時說明執行情形。

四、副本抄送直轄市、縣（市）政府，另檢送「不動產經紀業個人資料管理外部稽核表」請加強宣導及查處安維計畫及處理方法執行情形，以落實消費者個人資料安全維護。

正本：中華民國不動產仲介經紀商業同業公會全國聯合會、中華民國不動產代銷經紀商業同業公會全國聯合會

副本：各直轄市政府地政局、縣(市)政府、本部地政司(地籍科)(均含附件)

電 2022/01/14 文
交 15:08:14 章

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、個人資料檔案及資料庫之存取控制與保護監控措施。五、防止外部網路入侵對策。六、非法或異常使用行為之監控與因應機制。前項第五款及第六款所定措施，應定期演練及檢討改善。」是以，公司（商號）有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之情形者，該資通訊系統應至少有上開六項資訊安全措施。
- 二、為利實作，爰參考《資通安全責任等級分級辦法》（附表十）資通系統防護基準就上開6項資訊安全措施說明如下，以供公司（商號）之資訊人員，或資通訊系統之建置廠商參考：

資通系統防護基準實作說明

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、停用及刪除之程序，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	個人資料檔案及資料庫之存取控制與保護監控措施	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與因應機制	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。

不動產經紀業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、管理人員及資源				
(一)是否至少配置1名管理人員，負責規劃、訂定、修正與執行個人資料檔案安全維護計畫（以下簡稱安維計畫）及業務終止後個人資料處理方法（以下簡稱處理方法）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，並公告於營業處所適當之處或網站，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與清查				
是否定期查核確認所保有之個人資料現況，並界定納入安維計畫及處理方法之範圍？				
三、風險評估及管理機制				
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、事故之預防、通報及應變機制				
(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「矯正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達1,000筆以上時，應於發現後72小時內，以書面通報地方主管機關，並副知內政部之機制？				
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				

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)是否訂定並執行利用個人資料行銷時，明確告知當事人所屬公司(商號)名稱之規範？				
(四)是否訂定並執行加盟經營者利用個人資料行銷時，應告知加盟品牌名稱及公司(商號)名稱之規範？				
(五)是否訂定並執行利用個人資料行銷時，提供當事人免費表示拒絕接受行銷方式之規範？				
(六)是否訂定並執行當事人表示拒絕接受行銷時，應立即停止利用其個人資料行銷之規範？				
(七)是否訂定並執行當事人表示拒絕接受行銷之日起7日內，直營店應通知總公司(商號)彙整後再周知所屬各部門之規範？				
(八)是否訂定並執行當事人表示拒絕接受行銷之日起7日內，加盟店應通知內部其他業務人員，其有上傳加盟總部者，亦應併同通知加盟總部之規範？				
(九)是否訂定並執行當事人表示拒絕接受行銷之日起7日內，涉有參與聯賣服務者，應通知其他聯賣業者之規範？				
(十)是否訂定並執行中央主管機關對經紀業為限制國際傳輸個人資料之命令或處分時，通知所屬人員遵循辦理之規範？				
(十一)是否訂定並執行將個人資料作國際傳輸者，應檢視是否受中央主管機關限制，並告知當事人其個人資料所欲國際傳輸之區域之規範？				
(十二)是否訂定並執行將個人資料作國際傳輸時，對資料接收方為下列事項之監督之規範： 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. 當事人行使本法第3條所定權利之相關事項。				

稽核項目	辦理情形			發現說明
	是	否	不適用	
(十三)是否訂定並執行受理當事人依本法第3條行使個資各項權利時，應提供當事人行使個資各項權利時之聯絡窗口、聯絡方式之規範？				
(十四)是否訂定並執行受理當事人依本法第3條行使個資各項權利時，應驗證申請人身分為當事人本人或經授權之代理人之機制？				
(十五)除有妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益、本公司（商號）或第三人之重大利益等情形外，是否有依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本（本法第10條但書）？同意或拒絕當事人行使權利之事由，是否於法定期限內或法定延長期限內以書面通知當事人（15/30天）？				
(十六)是否訂定並執行個人資料正確性有爭議時，應主動或依當事人之請求停止處理或利用之規範？未主動或未依當事人之請求停止處理或利用時（本法第11條第2項但書），是否係因執行業務所必須或經當事人書面同意，並經註明其爭議？同意或拒絕當事人行使權利之事由，是否於法定期限內或法定延長期限以書面通知當事人（本法第13條：30/60天）？				
(十七)個人資料蒐集之特定目的消失或期限屆滿時，未主動或未依當事人之請求，刪除、停止處理或利用該個人資料時（本法第11條第3項但書），是否係因執行業務所必須或經當事人書面同意？同意或拒絕當事人行使權利之事由，是否於法定期限內或法定延長期限內以書面通知當事人（本法第13條：30/60天）？				
(十八)是否有訂定並執行當事人查詢、請求閱覽個人資料或製給複製本，有收取必要成本費用者，應告知當事人收費基準之規範？				
(十九)委託他人蒐集、處理或利用個人資料之全部或一部時，是否依本法施行細則第8條規定，與受託者明確約定相關監督事項及方式，並為適當之監督？				

稽核項目	辦理情形			發現說明
	是	否	不適用	
六、資料安全管理及人員管理				
(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？				
七、認知宣導及教育訓練				
(一)是否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？				

稽核項目	辦理情形			發現說明
	是	否	不適用	
(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，並指定適當人員每半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，並由公司(商號)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？				
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				

稽核項目	辦理情形			發現說明
	是	否	不適用	
(一)是否依公司(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)是否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？是否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？				
(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？				

不動產經紀業名稱：

公司(商號)查核人簽章：

公司(商號)負責人簽章：

不動產經紀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、管理人員及資源				
(一)是否至少配置1名管理人員，負責規劃、訂定、修正與執行個人資料檔案安全維護計畫(以下簡稱安維計畫)及業務終止後個人資料處理方法(以下簡稱處理方法)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，並公告於營業處所適當之處或網站，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與清查				
是否定期查核確認所保有之個人資料現況，並界定納入安維計畫及處理方法之範圍？				
三、風險評估及管理機制				
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、事故之預防、通報及應變機制				
(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「矯正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達1,000筆以上時，應於發現後72小時內，以書面通報地方主管機關，並副知內政部之機制？				
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				

稽核項目	辦理情形			發現說明
	是	否	不適用	
(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)是否訂定並執行利用個人資料行銷時，明確告知當事人所屬公司(商號)名稱之規範？				
(四)是否訂定並執行加盟經營者利用個人資料行銷時，應告知加盟品牌名稱及公司(商號)名稱之規範？				
(五)是否訂定並執行利用個人資料行銷時，提供當事人免費表示拒絕接受行銷方式之規範？				
(六)是否訂定並執行當事人表示拒絕接受行銷時，應立即停止利用其個人資料行銷之規範？				
(七)是否訂定並執行當事人表示拒絕接受行銷之日起7日內，直營店應通知總公司(商號)彙整後再周知所屬各部門之規範？				
(八)是否訂定並執行當事人表示拒絕接受行銷之日起7日內，加盟店應通知內部其他業務人員，其有上傳加盟總部者，亦應併同通知加盟總部之規範？				
(九)是否訂定並執行當事人表示拒絕接受行銷之日起7日內，涉有參與聯賣服務者，應通知其他聯賣業者之規範？				
(十)是否訂定並執行中央主管機關對經紀業為限制國際傳輸個人資料之命令或處分時，通知所屬人員遵循辦理之規範？				
(十一)是否訂定並執行將個人資料作國際傳輸者，應檢視是否受中央主管機關限制，並告知當事人其個人資料所欲國際傳輸之區域之規範？				

稽核項目	辦理情形			發現說明
	是	否	不適用	
(十二)是否訂定並執行將個人資料作國際傳輸時，對資料接收方為下列事項之監督之規範： 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. 當事人行使本法第3條所定權利之相關事項。				
(十三)是否訂定並執行受理當事人依本法第3條行使個資各項權利時，應提供當事人行使個資各項權利時之聯絡窗口、聯絡方式之規範？				
(十四)是否訂定並執行受理當事人依本法第3條行使個資各項權利時，應驗證申請人身分為當事人本人或經授權之代理人之機制？				
(十五)除有妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益、本公司(商號)或第三人之重大利益等情形外，是否有依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本(本法第10條但書)？同意或拒絕當事人行使權利之事由，是否於法定期限內或法定延長期限內以書面通知當事人(15/30天)？				
(十六)是否訂定並執行個人資料正確性有爭議時，應主動或依當事人之請求停止處理或利用之規範？未主動或未依當事人之請求停止處理或利用時(本法第11條第2項但書)，是否係因執行業務所必須或經當事人書面同意，並經註明其爭議？同意或拒絕當事人行使權利之事由，是否於法定期限內或法定延長期限以書面通知當事人(本法第13條：30/60天)？				
(十七)個人資料蒐集之特定目的消失或期限屆滿時，未主動或未依當事人之請求，刪除、停止處理或利用該個人資料時(本法第11條第3項但書)，是否係因執行業務所必須或經當事人書面同意？同意或拒絕當事人行使權利之事由，是否於法定期限內或法定延長期限內以書面通知當事人(本法第13條：30/60天)？				

稽核項目	辦理情形			發現說明
	是	否	不適用	
(十八)是否有訂定並執行當事人查詢、請求閱覽個人資料或製給複製本，有收取必要成本費用者，應告知當事人收費基準之規範？				
(十九)委託他人蒐集、處理或利用個人資料之全部或一部時，是否依本法施行細則第8條規定，與受託者明確約定相關監督事項及方式，並為適當之監督？				
六、資料安全管理及人員管理				
(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？				
七、認知宣導及教育訓練				
(一)是否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				

稽核項目	辦理情形			發現說明
	是	否	不適用	
(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，並指定適當人員每半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，並由公司(商號)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？				
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？				

稽核項目	辦理情形			發現說明
	是	否	不適用	
(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) 是否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？是否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？				
(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？				

不動產經紀業名稱：

個人資料專責管理人簽章：

不動產經紀業個人資料管理內部自主稽核檢核表法規依據及說明

稽核項目	依據條文	說明
一、管理人員及資源		
(一)是否至少配置1名管理人員，負責規劃、訂定、修正與執行個人資料檔案安全維護計畫（以下簡稱安維計畫）及業務終止後個人資料處理方法（以下簡稱處理方法）等相關事項，並定期向負責人提出報告？	第5條第1項	業者應指定至少1名管理人員並提出定期向負責人提出報告之證明文件。
(二)是否訂定個人資料保護管理政策，並公告於營業處所適當之處或網站，使其所屬人員及個人資料當事人均能知悉？	第5條第2項	業者應提供個人資料保護管理政策文件及於營業處所或網站揭示之相片或截圖。
二、個人資料之範圍界定與清查		
是否定期查核確認所保有之個人資料現況，並界定納入安維計畫及處理方法之範圍？	第6條	業者應提供所保有之個人資料現況、界定納入安維計畫及處理方法之範圍及定期查核紀錄。
三、風險評估及管理機制		
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？	第7條	業者應提供個資風險評估及管控措施文件。
四、事故之預防、通報及應變機制		
(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「矯正預防措施之研議機制」？	第8條第1項	業者應提供符合規定之應變、通報及預防機制文件。
(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」？	第8條第1項	業者應提供符合規定之應變措施文件。
(三) 是否訂定並執行個人資料事故達1,000筆以上時，應於發現後72小時內，以書面通報地方主管機關，並副知內政部之機制？	第8條第2項	業者可提供相關流程規範。
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	第9條	業者可提供相關流程規範。並應提供已要求所屬

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項但書情形?		人員確實辦理,或依規定執行之切結文件。
(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?	第10條	業者可提供符合規定之相關流程規範。並應提供已要求所屬人員確實辦理或依規定執行之切結文件。
(三)是否訂定並執行利用個人資料行銷時,明確告知當事人所屬公司(商號)名稱之規範?	第11條第1項	業者可提供符合規定之相關流程規範。並應提供已要求所屬人員、加盟店、直營店、聯賣業者,確實辦理或依規定執行之切結文件。
(四)是否訂定並執行加盟經營者利用個人資料行銷時,應告知加盟品牌名稱及公司(商號)名稱之規範?	第11條第1項	
(五)是否訂定並執行利用個人資料行銷時,提供當事人免費表示拒絕接受行銷方式之規範?	第11條第2項	
(六)是否訂定並執行當事人表示拒絕接受行銷時,應立即停止利用其個人資料行銷之規範?	第11條第3項	
(七)是否訂定並執行當事人表示拒絕接受行銷之日起7日內,直營店應通知總公司(商號)彙整後再周知所屬各部門之規範?	第11條第4項及第5項	
(八)是否訂定並執行當事人表示拒絕接受行銷之日起7日內,加盟店應通知內部其他業務人員,其有上傳加盟總部者,亦應併同通知加盟總部之規範?	第11條第4項及第5項	
(九)是否訂定並執行當事人表示拒絕接受行銷之日起7日內,涉有參與聯賣服務者,應通知其他聯賣業者之規範?	第11條第4項及第5項	
(十)是否訂定並執行中央主管機關對經紀業為限制國際傳輸個人資料之命令或處分時,通知所屬人員遵循辦理之規範?	第12條第1項	業者可提供符合規定之相關流程規範。並應提供已要求所屬人員確實辦理或依規定執行之切結文件。
(十一)是否訂定並執行將個人資料作國際傳輸者,應檢視是否受中央主管機關限制,並告知當事人其個人資料所欲國際傳輸之區域之規範?	第12條第2項	業者可提供符合規定之相關流程規範。並另提供告知當事人之個人資料所欲國際傳輸之區域之相關證明資料。如無則免提供。
(十二)是否訂定並執行將個人資料作國際傳輸時,對資料接收方為下列事項之監督之規範: 1. 預定處理或利用個人資料之範圍、類別、	第12條第2項	業者應提供傳輸前,提醒資料接收方受監督事項之文件。

<p>特定目的、期間、地區、對象及方式。</p> <p>2. 當事人行使本法第3條所定權利之相關事項。</p>		
<p>(十三)是否訂定並執行受理當事人依本法第3條行使個資各項權利時，應提供當事人行使個資各項權利時之聯絡窗口、聯絡方式之規範？</p>	<p>第 13 條 第1款</p>	<p>業者可提供符合規定之相關流程規範或教材。並應提供已要求所屬人員確實辦理或依規定執行之切結文件。</p>
<p>(十四)是否訂定並執行受理當事人依本法第3條行使個資各項權利時，應驗證申請人身分為當事人本人或經授權之代理人之機制？</p>	<p>第 13 條 第2款</p>	<p>業者可提供符合規定之相關流程規範或教材。並應提供已要求所屬人員確實辦理或依規定執行之切結文件。</p>
<p>(十五)除有妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益、本公司（商號）或第三人重大利益等情形外，是否有依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本（本法第10條但書）？同意或拒絕當事人行使權利之事由，是否於法定期限內或法定延長期限內以書面通知當事人(15/30天)？</p>	<p>第 13 條 第3款及 第5款</p>	<p>業者應提供實際案例回復文件（並檢視是否於法定期限內以書面通知）或制式空白回復文件。</p>
<p>(十六)是否訂定並執行個人資料正確性有爭議時，應主動或依當事人之請求停止處理或利用之規範？未主動或未依當事人之請求停止處理或利用時（本法第11條第2項但書），是否係因執行業務所必須或經當事人書面同意，並經註明其爭議？同意或拒絕當事人行使權利之事由，是否於法定期限內或法定延長期限以書面通知當事人(本法第13條：30/60天)？</p>	<p>第 13 條 第3款及 第5款</p>	<p>業者應提供當事人書面同意書、實際案例回復文件（並檢視是否於法定期限內以書面通知）或制式空白回復文件。</p>
<p>(十七)個人資料蒐集之特定目的消失或期限屆滿時，未主動或未依當事人之請求，刪除、停止處理或利用該個人資料時（本法第11條第3項但書），是否係因執行業務所必須或經當事人書面同意？同意或拒絕當事人行使權利之事由，是否於法定期限內或法定延長期限內以書面通知當事人(本法第13條：30/60天)？</p>	<p>第 13 條 第3款及 第5款</p>	<p>業者應提供當事人書面同意書、實際案例回復文件（並檢視是否於法定期限內以書面通知）或制式空白回復文件。</p>

(十八)是否有訂定並執行當事人查詢、請求閱覽個人資料或製給複製本，有收取必要成本費用者，應告知當事人收費基準之規範？	第 13 條 第4款	業者可提供實際案例經當事人署名之告知文件，或制式空白告知文件（含當事人簽名欄），或經所屬人員切結執行之流程規範。
(十九)委託他人蒐集、處理或利用個人資料之全部或一部時，是否依本法施行細則第8條規定，與受託者明確約定相關監督事項及方式，並為適當之監督？	第 21 條 第1項及 第2項	業者應提供與受託者明確約定相關監督事項之文件。
六、資料安全管理及人員管理		
(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？	第 15 條 第2項第 1款	業者應提供所屬人員存取權限定期設定文件。
(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？	第 15 條 第2項第 2款	業者應提供依業務性質制定之流程及其負責人員之規範文件。
(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？	第 15 條 第2項第 3款	業者應提供與所屬人員約定儲存媒介物保管及本項約定之切結書。
(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？	第 15 條 第2項第 4款	業者應提供與所屬人員本項約定之切結書。
(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？	第 16 條 第1項第 1款至第 4款	業者應提供相關機制文件。
(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？	第 16 條 第1項第 5款及第 6款、第 2項	業者應提供相關機制文件及定期演練紀錄及檢討改善等文件。
七、認知宣導及教育訓練		
(一)是否定期或不定期對於所屬人員施以基礎	第17條	業者可提供相關宣導及教

個人資料保護認知宣導及教育訓練？		育訓練資料。
(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？	第17條	業者可提供所屬人員考試成績或參訓人員名冊或切結書等。
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？	第 14 條 第1項及 第2項	業者可現場展示安全設備或防護措施。例如保險櫃及安全防護或加密機制等。
(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？	第 14 條 第2項第 2款	業者可現場展示。
(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？	第 14 條 第2項第 3款	業者可提供個資存放媒介物等報廢汰換或轉作其他用途時之措施或流程規範、文件。
(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。	第 14 條 第2項第 3款及第 21條	業者可提供委託他人蒐集、處理或利用個人資料、或委託他人將個人資料存放媒介物執行報廢汰換或轉作其他用途時，與受託者明確約定相關監督事項之文件。
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，並指定適當人員每半年至少進行一次安維計畫及處理方法執行情形之檢查？	第 18 條 第1項	業者應指定適當人員並提供至少每半年1次安維計畫及處理方法執行情形之稽核紀錄。
(二)是否將檢查結果向負責人提出報告，並由公司(商號)負責人於紀錄確認。上開相關紀錄並應留存至少五年？	第 18 條 第2項	業者可提供負責人簽名之稽核紀錄文件。
(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？	第 18 條 第3項	業者可提供不符時之改善文件，無不符之情形者免提供。經查有不符之情形者，應立即改善。
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	第 19 條	業者可提供個人資料刪

資料或相關證據。	第1項	除、停止處理或利用之方法、時間或地點之程序、措施等機制或文件。
(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？	第 19 條 第2項第 1款及第 3款	業者可提供個人資料刪除、停止處理或利用之方法、時間或地點之程序、措施等機制之文件。
(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？	第 19 條 第2項第 2款及第 3款	業者可提供符合規定之相關流程規範。業者可提供個人資料移轉其他對象時之措施、流程規範文件。
十一、個人資料安全維護計畫與整體持續改善		
(一)是否依公司(商號)之規模、特性、保有個人資料之性質及數量等事項，訂定適當之安維計畫？	第4條	檢視所訂之安維計畫是否適當。
(二)是否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？是否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？	第 20 條 及 第 23 條	檢視安維計畫是否依相關因素進行訂修，並於規定時間內報備查。
(三)是否訂定業務終止後，所保有個人資料銷毀之方法、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？	第22條	業者可提供符合規定之相關流程規範。並檢視處理方法是否依規定訂定。

註：本自主稽核表所列依據條文僅列《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》，所涉本法(個人資料保護法)部分請自行比對照辦。