

德信綜合證券股份有限公司

個人資料檔案安全維護計畫及業務終止後個人資料處理辦法

103 年 3 月 18 日 訂 定

106 年 8 月 28 日 第一次修正

第一章 總則

第1條

本計畫及處理方法依個人資料保護法(以下簡稱個資法)第27條、金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法第3條訂定之。

第2條

依個資法第2條之定義所適用的資料，係指自然人之姓名、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、社會活動及其他得以直接或間接方式識別該個人之資料。

第3條

本公司為規範個人資料之蒐集、處理及利用，並落實個人資料檔案之安全維護與管理，以防止個人資料被竊取、竄改、毀損、滅失或洩露，所應採取組織上與技術上適當之安全措施，應依本計畫及處理方法為之。

第二章 個人資料管理事項規劃

第一節 配置管理之人員及相當資源

第4條

本公司為執行策劃、訂定、執行、稽核與修訂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等相關個人資料管理事項，訂定個人資料保護組織及權限如下：

(一) 個人資料管理執行小組(下稱個資管理小組)

- 1、成員：總經理為召集人，小組成員含總管理部主管、經紀部主管、法令遵循室主管、資訊部主管與稽核室主管。
- 2、負責與管理個人資料保護管理制度執行與運作。
- 3、制訂相關規則及文件。
- 4、核決相關申請事宜。
- 5、任命相關人員。
- 6、向董事長報告個人資料保護管理制度之運作情形。
- 7、其他經董事會或董事長指派之工作。

(二) 稽核小組

- 1、成員：總公司稽核室及各分公司稽核。
- 2、制訂稽核作業流程及相關文件。

- 3、規劃及執行稽核作業。
- 4、向個資管理小組召集人報告稽核結果。
- 5、其他經個資管理小組指派之工作。

(三) 教育訓練小組

- 1、成員：法令遵循室主管。
- 2、制訂個人資料保護管理制度教育訓練計劃。
- 3、執行及管理員工教育訓練。
- 4、向個資管理小組報告教育訓練情形。
- 5、其他經個資管理小組指派之工作。

(四) 申訴諮詢小組

- 1、成員：客戶服務人員、交割主管。
- 2、建置當事人權利行使及申訴諮詢窗口。
- 3、追蹤當事人權利行使及申訴諮詢處理情形。
- 4、其他經個資管理小組指派之工作。

(五) 各部門及各分公司主管

- 1、管理所屬部門之個人資料。
- 2、監督所屬部門個人資料保護管理制度與客戶申辦資料、申訴諮詢之運作情形。
- 3、監督所屬部門安全管理措施之執行
- 4、其他經個資管理小組指派之工作。

第二節 界定個人資料範圍

第5條

本公司各個部門應清查所持有之個人資料，並製作個人資料盤點清冊，送交個資管理小組核決。盤點個人資料時應將個人資料名稱、特定目的、蒐集方法、保存場所、保存形態、保存期間、刪除銷毀方法等事項記載於清冊。個人資料盤點作業程序由個資管理小組訂定，並由總經理核定。

第三節 個人資料之風險評估及管理機制

第6條

個資管理小組與各部門負責人對於各部門保有之個人資料，應斟酌個人資料被且竊取、洩露、竄改或其他侵害、目的外利用等情形，進行風險評鑑，並製作風險分析清冊。

個資管理小組及各部門負責人對於評鑑結果應進行檢討，並擬訂風險管理機制。

第四節 事故之預防、通報及應變機制

第7條

本公司對於個人資料被竊取、竄改、毀損、滅失或洩露事故之處理，應就下列事項訂定緊急應變作業程序：

- (一) 通報對象與其通報方式。
- (二) 啟動緊急應變措施，控制當事人之損害。

- (三) 查明事實。
- (四) 執行因應措施。
- (五) 公告及通知當事人，包括事實原因、所為因應措施及諮詢服務專線等。
- (六) 防止事故再次發生之矯正預防措施。
- (七) 其他

本公司遇重大個人資料事故，應即通報金管會；並考慮向警察局等治安機關報案。所研議之矯正預防措施應經公正、獨立且取得相關公認認證資格之專家，進行整體診斷及檢視。

前項所稱重大個人資料事故，係指個人資料遭竊取、竄改、毀損、滅失或洩露，將危及本公司正常營運或大量關係人權益之情形。

第五節 認知宣導及教育訓練

第8條

教育訓練小組擬訂本公司個人資料教育訓練計劃，其內容應包括以下事項：

- (一) 時程
- (二) 對象
- (三) 內容
- (四) 執行
- (五) 成果
- (六) 檢討

前項計劃應送請個資管理小組核決，修正時亦同。

第三章 個人資料蒐集、處理及利用之內部管理程序

第9條

有關醫療、基因、性生活、健康檢查及犯罪前科等特種個人資料，除符合法定情形外，不得蒐集、處理或利用。

本公司有關特種個人資料之蒐集、處理或利用，由各部門提出申請，經個資管理小組核決後，依蒐集、處理、利用程序為之。

第10條

一、蒐集

各部門於執行業務而有蒐集個人資料時，應具有特定目的，並確認是否符合下列情形之一：

- (一) 法律明文規定。
- (二) 與當事人有契約或類似契約之關係，且已採取適當之安全措施。
- (三) 當事人自行公開或其他已合法公開之個人資料。
- (四) 學術研判機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。
- (五) 經當事人同意。
- (六) 為增進公共利益所必要。

(七) 個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益，不在此限。

(八) 對當事人權益無侵害。

各部門負責人應依據法務部頒訂「個人資料保護法之特定目的及個人資料之類別」確定符合該部門蒐集個人資料之特定目的，並送請個資小組核決，有增加或刪除時亦同。

二、處理

各部門應先設定處理權限範圍，並於處理個人資料時，應先確定是否符合特定目的並具備前項一定情形之一。

第11條

各部門依前條規定蒐集個人資料時，除符合第2 項而免為告知時，應明確告知當事人下列事項：

- (一) 本公司名稱。
- (二) 蒐集之目的。
- (三) 個人資料之類別。
- (四) 個人資料利用之期間、地區、對象及方式。
- (五) 當事人依第三條規定得行使之權利及方式。
- (六) 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。

有下列情形之一者，本公司得免為前項之告知：

(一) 直接向當事人蒐集時：

- 1、依法律規定得免告知。
- 2、個人資料之蒐集係履行法定義務所必要。
- 3、告知將妨害公務機關執行法定職務。
- 4、告知將妨害公共利益。
- 5、當事人明知應告知之內容。
- 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。

(二) 間接向當事人蒐集時：

- 1、有前款所列情形之一。
- 2、當事人自行公開或其他已合法公開之個人資料。
- 3、不能向當事人或其法定代理人為告知。
- 4、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。
- 5、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。

第12條

本公司全體員工應於達成特定目的之必要範圍內利用所蒐集、處理之個人資料；於利用時，對於是否逾越特定目的之必要範圍產生疑義，應由該部門負責人向個資管理小組提出確認申請，並由個資小組做成決定後通知該部門。

各部門為特定目的外利用個人資料時，除須經符合下列情形之一外，並應向個資

小組提出申請，經個資小組核決後方得為之：

- (一) 法律明文規定。
- (二) 為增進公共利益所必要。
- (三) 為免除當事人之生命、身體、自由或財產上之危險。
- (四) 為防止他人權益之重大危害。
- (五) 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。
- (六) 經當事人同意。
- (七) 有利於當事人權益。

第13條

本公司委託他人蒐集、處理或利用個人資料時，應依下列程序為之：

- (一) 由個資管理小組訂定委外廠商選擇標準。
- (二) 各部門進行委外時，應先了解委外場商有關個人資料保護政策及執行情形，並記錄於委外廠商評鑑表，評估是否符合本公司委外廠商選擇標準。
- (三) 依本公司委外廠商選擇標準選定委外廠商後，應送請個資管理小組核決。
- (四) 本公司應與委外廠商簽訂委外契約，並應記載下列事項：
 - 1、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。
 - 2、有複委託者，其約定之受託者。
 - 3、受託者或其受僱人違反個資法、其他個人資料保護法律或其法規命令時，應向本公司通知之事項及採行之補救措施。
 - 4、本公司如對受託者有保留指示者，其保留指示之事項。
 - 5、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。
 - 6、其他經個資管理小組認為有必要記載之事項。
- (五) 本公司應定期確認受託者執行之狀況，並將確認結果記錄之。

第14條

員工利用個人資料為首次行銷時，應於該次行銷中以當時行銷之方式(書面、口頭或其他方式行銷)，表明當事人得以免費方式表示拒絕接受行銷(當場表示、以免付費電話或免付費回郵等方式)。

當事人表示拒絕接受行銷者，本公司應停止利用該個人資料進行行銷，並於該當事人檔案中註明後通知個資管理小組，由個資管理小組以適當方式確保該當事人之個人資料不再做為行銷之用。

第15條

各部門進行個人資料國際傳輸前，應確認中央目的事業主管機關是否有國際傳輸之限制規定。

第16條

當事人依法得向本公司行使下列權利：

- (一) 查詢或請求閱覽。

- (二) 請求製給複製本。
- (三) 請求補充及更正
- (四) 請求停止蒐集、處理或利用。
- (五) 請求刪除。

當事人本人向本公司行使第1項所列權利時，應提出權利行使申請書，並出示身份證、駕照等其他足資證明其身份之證明以供查驗。若由法定代理人提出申請，應再提出其身份證件及授權書。

本公司受理當事人行使查詢、閱覽、製給複製本申請後，應於十五日內為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。

本公司受理當事人行使更正、補充、請求刪除、停止蒐集、處理、或利用後，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。

本公司於受理當事人前項申請後，經審查後認為有符合個人資料保護法第10條第1項但書、第11條第2項及第3項情形時，得做成駁回之決定。

當事人查詢或請求閱覽個人資料或製給複本者，本公司得酌收必要成本費用，其費率由個資管理小組訂定。

第17條

本公司員工於個人資料蒐集、處理或利用時，應以適當方法確認當事人個人資料之正確性；若發現有錯誤時，應以適當方式更正或補充。

因可歸責於本公司之事由未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用對象。

個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行業務所必須並註明其爭議或經當事人書面同意者，不在此限。

第18條

各部門因辦理相關業務而蒐集之個人資料，於特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理及利用該個人資料。但因執行業務所必須或經當事人書面同意者，不在此限。

第四章 個人資料管理措施

第19條

為防止個人資料發生被竊取、竄改、毀損、滅失或洩漏等遭受侵害之情事，應依本章規定辦理。

第一節 資料安全管理、人員管理及業務終止後個人資料處理方法

第20條

本公司因執行業務所保有個人資料安全，應採取下列管理措施：

- (一) 對於個人資料之蒐集、處理及利用，應依本計畫及處理方法第三章規定辦理。

- (二) 本公司對於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，應就使用可攜式設備或儲存媒體之管理，由資訊部訂定相關作業程序。
- (三) 針對所保有之個人資料內容，如有加密之必要，於蒐集、處理或利用時，宜採取適當之加密機制。
- (四) 作業過程有備份個人資料之必要時，應比照原件個人資料安全措施方式予以保護。
- (五) 個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物，嗣該等媒介物報廢或做其他用途時，應採取適當防範措施；若委託他人執行上開行為時，宜依本辦法第12 條規定辦理。
- (六) 本公司提供電子商務服務系統，應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. 應用系統於開發、上線、維護等各階段軟體驗證與確認程序。
 5. 個人資料檔案及資料庫之存取控制與保護監控措施。
 6. 防止外部網路入侵對策。
 7. 非法或異常使用行為之監控與因應機制。

第21條

各部門負責人應設定得接觸個人資料之權限，並載明於個人資料管理人員權限表，並要求員工嚴格保守秘密。

前項個人資料管理人員權限表由各部門負責人製作，並送請個資小組核決。

第22條

各部門對於超過保存年限而應銷毀之個人資料，應先報請個資管理小組核備後，以適當方式銷毀至無法辨識之程度。

前項應銷毀之個人資料逾100 筆者，該部門負責人應指派二人共同辦理。

承辦銷毀人員應將個人資料檔案名稱、銷毀方法、時間及方式記錄並留存。

第二節 設備安全管理

第23條

處理及儲存個人資料之各項設備應安置於適當之安全處所，並指派專人進行管理，以維護個人資料之安全。

因進行前項安全管理所為之管制作業應做成記錄，個資管理小組應不定期檢查管制記錄。

資訊部門應定期檢討及評估有關電子資料安全之各項軟、硬體設備之安全性，確保得以正確且有效執行安全措施。

第五章 個人資料安全稽核、記錄保存及改善機制

第一節 資料安全稽核機制

第24條

為符合個人資料保護法之要求，並為確認個人資料保護管理制度適當運作，稽核小組應定期(每半年)對各部門實施內部稽核，稽核小組如認為有必要時，亦得隨時進行內部稽核。

前項稽核作業程序由稽核小組訂定，並送請個資管理小組核決。

第二節 使用紀錄、軌跡資料及證據保存

第25條

以下資料屬於個人資料保護管理制度之重要文件：

- (一) 個人資料檔案安全維護計畫及業務終止後個人資料處理辦法。
- (二) 個人資料保護管理相關管理規則或作業流程。
- (三) 其他實行個人資料保護制度所製作之文件。

文件原本依種類保存於各部門檔案櫃中，並由個資管理小組指定管理人。

為進行文件及其紀錄管理，個資管理小組應製作文件一覽表及紀錄管理一覽表。文件一覽表應包括文件名稱、製訂日、修訂日、核決人、保存場所等事項。紀錄管理一覽表應包括使用文件名稱、核決人、保存場所、保存期間、保存負責人等事項。

文件管理人應定期將超過保存期限之紀錄廢棄之，若依法令規定或個資管理小組任有繼續保存之必要者，應另為適當之處理，並應留存下列紀錄：

- (一) 刪除、停止處理或利用之方法、時間。
- (二) 將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。

前二項之軌跡資料、相關證據及紀錄，應至少留存五年。但法令另有規定或契約另有約定者，不在此限。

第三節 個人資料安全維護之整體持續改善

第26條

個資管理小組應依下列步驟，定期檢視及修訂本計畫及處理辦法：

- (一) 蒐集最新法令及相關實務見解。
- (二) 參考各部門個人資料保護管理制度運作情形及稽核報告。
- (三) 召開個人資料保護管理制度檢視修訂會議，並做成會議紀錄。
- (四) 執行及追蹤檢視修訂後之措施。

第27條

各部門之稽核結果有不符合之事項或具有違反法令之風險者，應依下列步驟儘速執行矯正預防措施：

- (一) 由個資管理小組及各部門負責人確認不符合之事項或具有違反法令風險之內容。
- (二) 各部門負責人清查其原因及提出矯正預防措施方法。
- (三) 個資管理小組核決所提出之矯正預防措施方法。
- (四) 各部門負責人執行矯正預防措施。
- (五) 紀錄其執行結果並製作矯正預防措施報告書，送請個資管理小組核決。

第六章 附則

第28條

本計畫及處理辦法經董事會決議後實施，修正時亦同。