法規名稱：票據交換所個人資料檔案安全維護計畫標準辦法

修正日期：民國 113 年 06 月 27 日

第 一 章 總則

第 1 條

本辦法依個人資料保護法（以下簡稱本法）第二十七條第二項及第三項規定訂定之。

第 2 條

1 票據交換所應訂定個人資料檔案安全維護計畫（以下簡稱本計畫），以落實個人資料檔案之安全維護與管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

2 本計畫之內容應包括第四條至第二十七條規定之相關組織及程序。

第 3 條

本辦法用詞定義如下：

一、個人資料管理代表：由票據交換所總經理擔任，或由總經理直接授權，負責督導本計畫之規劃、訂定、執行、修訂及相關決策之人員。

二、個人資料內評代表：由票據交換所總經理授權，負責督導相關內評人員評核本計畫之執行成效之人員。

三、所屬人員：執行業務之過程必須接觸個人資料之人員，包括票據交換所之定期或不定期契約人員及派遣員工。

第 4 條

1 票據交換所應建立個人資料檔案安全維護管理組織，並配置相當資源，負責本計畫相關程序之規劃、訂定、執行與修訂等任務。

2 個人資料檔案安全維護管理組織之成員應包括個人資料管理代表及個人資料內評代表。

3 個人資料管理代表非由總經理擔任時，應定期就個人資料檔案安全維護管理組織執行任務情形向總經理提出書面報告。

第 二 章 一般程序

第 5 條

1 票據交換所應依其組織與事業特性訂定個人資料保護管理政策，提報董事會通過，並公開周知，使其所屬人員均明確瞭解及遵循。

2 前項管理政策至少應包括下列事項之說明：

一、遵守我國個人資料保護相關法令規定。

二、以合理安全之方式，於特定目的範圍內，蒐集、處理及利用個人資料。

三、以可期待之合理安全水準技術保護其所蒐集、處理、利用之個人資料檔案。

四、設置聯絡窗口，供個人資料當事人行使其個人資料相關權利或提出相關申訴與諮詢。

五、規劃緊急應變程序，以處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故。

六、如委託蒐集、處理及利用個人資料者，應妥善監督受託機關。

七、持續維運本計畫之義務，以確保個人資料檔案之安全。

第 6 條

票據交換所應定期檢視應遵循之個人資料保護法令，並據以訂定或修訂本計畫。

第 7 條

票據交換所應依個人資料保護法令，清查所保有之個人資料，界定其納入本計畫之範圍並建立清冊，且定期確認其變動情形。

第 8 條

票據交換所應依據前條界定之個人資料範圍及其相關業務流程，分析可能產生之風險，並依據風險分析結果，訂定適當管控措施。

第 9 條

1 票據交換所為因應其保有之個人資料被竊取、竄改、毀損、滅失或洩漏等事故，應就下列事項建立相關程序：

一、採取適當之應變措施，以降低或控制事故對當事人之損害。

二、查明事故之狀況並適時通知當事人，通知內容應包含個人資料發生事故之事實、採取之因應措施及所提供之諮詢服務專線。

三、避免類似事故再次發生。

2 票據交換所遇有前項事故時，應即以電話通報中央銀行（以下簡稱本行）受理通報專責人員，並於三十六小時內，依附表格式，以電子郵件傳送本行。但有下列情形之一者，應即以電話通報，並即時依附表格式，以電子郵件傳送本行：

一、行政院、立法院或監察院關注之個人資料外洩案件。

二、經媒體顯著披露之個人資料外洩案件，例如經平面媒體全國性版面報導、電子媒體專題討論。

3 票據交換所應自前項電話通報日之次日起，於七個營業日內以書面方式將發生事故之事實、是否已遭不法利用、當事人權益受損情形及採取之因應措施等事項陳報本行。但有前項但書各款情形之一者，應於電話通報日之次營業日以書面方式陳報本行。

4 本行於接獲票據交換所通報後，得依本法第二十二條至第二十六條規定所賦予之職權，為適當之監督管理措施。

第 9-1 條

1 票據交換所應配合本行辦理下列事項：

一、本行每年辦理之個人資料保護行政檢查。

二、就前條第一項所定事故辦理之行政調查與複查。

2 前項行政檢查或行政調查與複查提列之應改善辦理事項，票據交換所應研提具體改善措施及後續處置情形函報本行。

第 三 章 法令遵循程序

第 10 條

票據交換所為確保個人資料之蒐集符合個人資料保護相關法令要求，應就下列事項建立相關程序：

一、確認蒐集個人資料之特定目的。

二、確認具備法令所要求之特定情形或其他要件。

第 11 條

票據交換所為遵守本法第八條及第九條有關蒐集個人資料之告知義務規定，應就下列事項建立相關程序：

一、確認是否得免告知。

二、除確認無須告知者外，應依據資料蒐集之情況，採取適當之告知方式。

第 12 條

票據交換所為確保個人資料之利用符合個人資料保護相關法令要求，應就下列事項建立相關程序：

一、確保個人資料之利用符合特定目的。

二、確認是否得進行及如何進行特定目的外利用。

第 13 條

票據交換所新增或變更特定目的時，應依下列程序為之：

一、依第十一條規定之程序為之。

二、取得當事人書面同意，但法令另有規定者，不在此限。

第 14 條

票據交換所針對本法第六條之特種個人資料，應就下列事項建立相關程序：

一、確認其蒐集、處理及利用之個人資料是否包含特種個人資料。

二、確保其蒐集、處理及利用特種個人資料，符合相關法令之要求。

第 15 條

票據交換所進行個人資料國際傳輸前，應確認是否受本行限制並遵循之。

第 16 條

票據交換所為提供個人資料當事人行使本法第三條規定之權利，應就下列事項建立相關程序：

一、如何提供當事人行使權利。

二、確認當事人身分。

三、確認是否有本法第十條及第十一條得拒絕當事人行使權利之情況。

四、適時准駁當事人請求。

第 17 條

1 票據交換所為確認其保有個人資料之正確性，應就下列事項建立相關程序：

一、確保資料於處理過程中，正確性不受影響。

二、當確認資料有錯誤時，應適時更正。

三、定期檢查資料之正確性。

2 因可歸責於票據交換所之事由，未為更正或補充之個人資料，應訂定於更正或補充後，通知曾提供利用對象之程序。

第 18 條

票據交換所應定期確認其所保有個人資料之特定目的是否消失，或期限是否屆滿，若特定目的消失或期限屆滿時，應遵守本法第十一條第三項規定。

第 四 章 安全管理措施

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，票據交換所應依據業務性質、個人資料存取環境、個人資料種類與數量及個人資料傳輸工具與方法等因素，採取第二十條至第二十三條之管理措施。

第 20 條

票據交換所應採取下列人員管理措施：

一、指定蒐集、處理及利用個人資料個別作業（以下簡稱「個別作業」）流程之負責人員。

二、就個別作業設定所屬人員不同之權限並控管之，以一定認證機制管理其權限，且定期確認權限內容設定之適當與必要性。

三、要求所屬人員負擔相關之保密義務。

第 21 條

票據交換所應採取下列作業管理措施：

一、訂定個別作業注意事項。

二、運用電腦及相關設備處理個人資料時，應訂定使用可攜式儲存媒體之規範。

三、儲存個人資料時，確認是否有加密之必要，如有必要，應採取適當之加密機制。

四、傳輸個人資料時，因應不同之傳輸方式，確認是否有加密之必要，如有必要，應採取適當之加密機制，並確認資料收受者之正確性。

五、應依據其保有資料之重要性，評估個人資料是否有備份必要，如有必要，應予備份。對於備份資料應確認是否有加密之必要，如有必要，應採取適當之加密機制，儲存備份資料之媒體，亦應以適當方式保管，且定期進行備份資料之還原測試，以確保備份之有效性。

六、儲存個人資料之媒體於廢棄或移轉與他人前，應確實刪除媒體中所儲存之資料，或以物理方式破壞之。

七、妥善保存認證機制及加密機制中所運用之密碼，如有交付他人之必要，亦應妥善為之。

第 22 條

票據交換所應採取下列物理環境管理措施：

一、依個別作業內容之不同，實施必要之門禁管理。

二、妥善保管個人資料之儲存媒體。

三、針對個別作業環境之不同，建置必要之防災設備。

第 23 條

票據交換所利用電腦或相關設備蒐集、處理或利用個人資料時，應採取下列技術管理措施：

一、於電腦、相關設備或系統上設定認證機制，對有存取個人資料權限之人員進行識別與控管。

二、認證機制使用帳號及密碼之方式時，使其具備一定安全之複雜度並定期更換密碼。

三、於電腦、相關設備或系統上設定警示與相關反應機制，以對不正常之存取為適當之反應與處理。

四、對於存取個人資料之終端機進行身分認證，以識別並控管之。

五、個人資料存取權限之數量及範圍，於個別作業必要之限度內設定之，且原則上不得共用存取權限。

六、採用防火牆或路由器等設定，避免儲存個人資料之系統遭受無權限之存取。

七、使用可存取個人資料之應用程式時，確認使用者具備使用權限。

八、定期測試權限認證機制之有效性。

九、定期檢視個人資料之存取權限設定正當與否。

十、於處理個人資料之電腦系統中安裝防毒軟體，並定期更新病毒碼。

十一、對於電腦作業系統及相關應用程式之漏洞，定期安裝修補之程式。

十二、定期瞭解惡意程式之威脅，並確認安裝防毒軟體及修補程式後之電腦系統之穩定性。

十三、具備存取權限之終端機不得安裝檔案分享軟體。

十四、測試處理個人資料之資訊系統時，不使用真實之個人資料，如使用真實之個人資料時，應明確規定其使用之程序。

十五、處理個人資料之資訊系統有變更時，應確認其安全性並未降低。

十六、定期檢查處理個人資料之資訊系統之使用狀況及個人資料存取之情形。

第 五 章 認知宣導及教育訓練

第 24 條

票據交換所應對所屬人員施以認知宣導及教育訓練，使其明瞭個人資料保護相關法令之要求、所屬人員之責任範圍及各種作業程序。

第 六 章 計畫稽核及改善程序

第 25 條

票據交換所為確保本計畫之有效性，應定期檢查本計畫是否落實執行。

第 26 條

為持續改善本計畫，票據交換所應建立下列程序：

一、本計畫發生未落實執行時之改善程序。

二、本計畫有變更時之變更程序。

第 七 章 紀錄機制

第 27 條

本計畫各項程序執行時，票據交換所至少應保存下列紀錄：

一、個人資料交付、傳輸之紀錄。

二、確認個人資料正確性及更正之紀錄。

三、提供當事人行使權利之紀錄。

四、個人資料刪除、廢棄之紀錄。

五、存取個人資料系統之紀錄。

六、備份及還原測試之紀錄。

七、所屬人員權限新增、變動及刪除之紀錄。

八、所屬人員違反權限行為之紀錄。

九、因應事故發生所採取行為之紀錄。

十、定期檢查處理個人資料之資訊系統之紀錄。

十一、教育訓練之紀錄。

十二、本計畫稽核及改善程序執行之紀錄。

第 八 章 施行日期

第 28 條

本辦法自發布日施行。