法規名稱：報關業個人資料檔案安全維護管理辦法
發布日期：民國 111 年 03 月 04 日
生效狀態：※本法規部分或全部條文尚未生效
本辦法除第 6 條自發布日施行外，自發布後六個月施行。

第 1 條

本辦法依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定之。

第 2 條

1 本辦法適用對象爲依關稅法第二十二條規定經海關許可設置之報關業（以下簡稱報關業）。
2 報關業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及管理措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
3 本計畫內容應包括第三條至第二十二條規定之相關組織及程序，並應定期檢視及配合相關法令修正。

第 3 條

1 報關業就個人資料檔案安全維護管理應指定專人或建立專責組織，並配置相當資源。
2 前項專人或專責組織之任務如下：
一、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。
二、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，公告使其所屬人員均明確瞭解。
三、定期對所屬人員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規定、所屬人員責任範圍及各種個人資料保護事項之方法或管理措施。
四、定期就執行任務情形向報關業代表人或經其授權人員提出書面報告。
3 本計畫之訂定或修正，應經報關業代表人或其授權人核定。

第 4 條

報關業應清查保有之個人資料，界定其納入本計畫之範圍並建立檔案，且應定期清查其有否變動。

第 5 條

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

第 6 條

1 報關業爲因應保有之個人資料被竊取、竄改、毀損、滅失或洩漏等安全事故，應採取下列措施：
一、採取適當應變措施，以控制事故對當事人之損害，並通報財政部關務署。
二、查明事故狀況並以適當方式通知當事人有關事實、因應措施及諮詢服務專線等。
三、研議預防機制，避免類似事故再次發生。
2 報關業遇有前項個人資料安全事故，應自發現事故時起算七十二小時內，檢附「個人資料侵害事故通報及紀錄表」（如附表），以電子郵件方式向財政部關務署通報，並應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關務署。
3 財政部關務署收受前項通報後，得依本法第二十二條至第二十五條規定所賦予之職權，爲適當監督管理措施。

第 7 條

報關業應依個人資料屬性，分別訂定下列管理程序：

一、確認蒐集、處理或利用之個人資料是否包含本法第六條所定個人資料及其特定目的。

二、確保蒐集、處理或利用本法第六條所定個人資料符合相關法令要件。

三、非本法第六條所定個人資料，如認爲具有特別管理需要，得訂定特別管理程序。

第 8 條

報關業爲遵守本法第八條及第九條關於告知義務規定，應採取下列方式：

一、檢視蒐集、處理或利用個人資料之特定目的，除符合法定免爲告知事由外，均應依法告知當事人相關事項。

二、依資料蒐集情況，採取適當告知方式。

第 9 條

1 報關業蒐集、處理個人資料應符合本法第十九條第一項規定，具有特定目的及法定要件。

2 報關業利用個人資料應依本法第二十條第一項規定，於特定目的內利用；於特定目的外利用個人資料時，應具備法定特定目的外利用要件。

第 10 條

報關業委託他人蒐集、處理或利用個人資料之全部或一部時，應對受託者依本法施行細則第八條規定爲適當之監督，並明確約定相關監督事項及方式。

第 11 條

1 報關業利用個人資料行銷，應符合本法第二十條第一項規定。

2 報關業依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。

3 報關業於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。

第 12 條

報關業進行個人資料國際傳輸，應遵循財政部依本法第二十一條規定所爲限制國際傳輸之命令或處分，並告知當事人其個人資料國際傳輸之區域，同時對資料接收方爲下列事項之監督：

一、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。

二、當事人行使本法第三條所定權利之相關事項。

第 13 條

報關業爲提供當事人行使本法第三條規定權利，應採取下列方式：

一、確認其爲個人資料之本人，或經個人資料之本人委託授權。

二、提供當事人行使權利之方式，並遵守本法第十三條有關處理期限規定。

三、如酌收必要成本費用應予告知。

四、具本法第十條但書及第十一條第二項但書、第三項但書規定得拒絕當事人行使權利之事由，應附理由通知當事人。

第 14 條

報關業爲維護保有個人資料之正確性，應採取下列方式：

一、於蒐集、處理或利用過程檢視個人資料正確性。

二、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。

三、個人資料正確性有爭議者，依本法第十一條第二項規定處理。

第 15 條

報關業應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，應依本法第十一條第三項規定處理。

第 16 條

報關業應採取下列人員管理措施：

一、依據作業需要，建立管理機制，設定所屬人員不同權限，並定期確認權限內容適當性及必要性。

二、指定各相關業務流程涉及蒐集、處理或利用個人資料之負責人員。

三、與所屬人員約定保密義務。

四、所屬人員離職時，持有之個人資料應辦理交接，不得於離職後繼續使用，並簽訂保密切結書。

第 17 條

報關業應採取下列資料安全管理措施：

一、運用電腦或自動化機器設備蒐集、處理或利用個人資料時，訂定使用可攜式設備或儲存媒體規範。

二、保有之個人資料內容如有加密需要，應於蒐集、處理或利用時，採取適當加密機制。

三、作業過程有備份個人資料需要時，比照原件，依本法規定予以保護。

四、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、電腦、自動化機器設備或其他存放媒介物報廢或轉作其他用途時，採取適當防範措施，以免由該媒介物洩漏個人資料。

第 18 條

1 報關業因執行業務以資通訊系統蒐集、處理或利用個人資料，且保有之個人資料達一萬筆者，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、非法或異常使用行爲之監控及因應機制。

2 報關業保有個人資料筆數未達一萬筆，於本條文施行後，因直接或間接蒐集而達一萬筆者，應於保有筆數達一萬筆之日起算六個月內採行前項資訊安全措施。

3 第一項第五款及第六款所定措施，應定期演練及檢討改善。

第 19 條

報關業保有之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、電腦或自動化機器設備等媒介物，應採取下列環境及設備安全管理措施：

一、針對存放儲存媒介物之環境，實施適當進出管制措施。

二、依儲存媒介物之特性及使用方式，建置適當保護設備或技術。

三、依所屬人員業務特性、內容及需求，訂定適當管理措施。

第 20 條

1 報關業應採行適當措施，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機制，以供必要時說明本計畫執行情況。

2 報關業對於業務終止後保有之個人資料，應依下列方式處理，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。

3 前二項紀錄、軌跡資料及相關證據，應至少留存五年。

第 21 條

報關業應訂定個人資料安全稽核機制，定期或不定期查察，以確保落實執行本計畫相關事項。

第 22 條

報關業應參酌執行業務現況、社會輿情、技術發展、法令修正等因素，檢視本計畫合宜性，必要時應予修正。

第 23 條

本辦法除第六條自發布日施行外，自發布後六個月施行。