法規名稱：公益彩券發行機構個人資料檔案安全維護管理辦法
修正日期：民國 110 年 07 月 28 日
生效狀態：※本法規部分或全部條文尚未生效
本辦法 110.07.28　增訂發布之第 17-1 條條文，自發布後三個月施行。

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 本辦法適用對象爲財政部指定擔任公益彩券之發行機構（以下簡稱發行機構）。
2 發行機構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。
3 本計畫之內容應包括第三條至第二十一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 發行機構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、處理及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之規定、所屬人員之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發行機構代表人或經其授權之人員提出書面報告。
3 本計畫之訂定或修正，應經發行機構代表人或經其授權之人員核定。

第 4 條

發行機構應清查所保有之個人資料，界定其納入本計畫之範圍並建立檔案，且定期確認其有否變動。

第 5 條

發行機構應依據前條所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，並依據風險分析之結果，訂定適當之管控措施。

第 6 條

1 發行機構爲因應所保有之個人資料被竊取、竄改、毀損、滅失或洩漏等事故，應採取下列措施：
一、適當之應變措施，以控制事故對當事人之損害，並通報有關單位。
二、查明事故之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 發行機構遇有個人資料安全事故者，應自事故發生時起算七十二小時內，依附表格式，以電子郵件通報財政部，並應視案情發展適時通報處理情形，以及將整體查處過程、結果與檢討等函報財政部。財政部於接獲發行機構通報後，得依本法第二十二條至第二十五條規定所賦予之職權，爲適當之監督管理措施。
3 發行機構遇有危及正常營運或大量當事人權益之重大個人資料安全事故，第一項預防機制應經公正、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。

第 7 條

發行機構應依個人資料之屬性，分別訂定下列管理程序：

一、檢視及確認所蒐集、處理及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、處理及利用本法第六條所定個人資料，是否符合相關法令之要件。

三、雖非本法第六條所定個人資料，惟如認爲具有特別管理之需要，仍得比照或訂定特別管理程序。

第 8 條

發行機構爲遵守本法第八條及第九條關於告知義務之規定，應採取下列方式：

一、檢視蒐集、處理個人資料之特定目的，是否符合免告知當事人之事由。

二、依據資料蒐集之情況，採取適當之告知方式。

第 9 條

1 發行機構應檢視蒐集、處理個人資料是否符合本法第十九條規定，具有特定目的及法定要件。

2 發行機構應檢視利用個人資料是否符合本法第二十條第一項規定，符合特定目的內利用；於特定目的外利用個人資料時，應檢視是否具備法定特定目的外利用要件。

第 10 條

發行機構委託他人蒐集、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與方式。

第 11 條

發行機構於首次利用個人資料行銷時，應提供當事人免費表示拒絕行銷之方式，且倘當事人表示拒絕行銷後，應立即停止利用其個人資料行銷，並週知所屬人員。

第 12 條

發行機構進行個人資料國際傳輸前，應檢視有無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，並應遵循之。

第 13 條

發行機構爲提供資料當事人行使本法第三條所規定之權利，應採取下列方式爲之：

一、確認是否爲個人資料之本人，或經其委託授權。

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之規定。

三、告知是否酌收必要成本費用。

四、如認有本法第十條及第十一條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

發行機構爲維護其所保有個人資料之正確性，應採取下列方式爲之：

一、檢視個人資料於蒐集、處理或利用過程是否正確。

二、當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，應依本法第十一條第二項規定處理。

第 15 條

發行機構應定期確認其所保有個人資料之特定目的是否消失及期限是否屆滿，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

發行機構應採取下列人員管理措施：

一、依據作業之需要，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之適當及必要性。

二、檢視各相關業務流程涉及蒐集、處理及利用個人資料之負責人員。

三、與所屬人員約定保密義務。

第 17 條

發行機構應採取下列資料安全管理措施：

一、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時，訂定使用可攜式設備或儲存媒體之規範。

二、針對所保有之個人資料內容，如有加密之需要，於蒐集、處理或利用時，採取適當之加密機制。

三、作業過程有備份個人資料之需要時，比照原件，依本法規定予以保護之。

四、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，嗣該媒介物於報廢或轉作其他用途時，採適當防範措施，以免由該媒介物洩漏個人資料。

第 17-1 條

1 發行機構因執行業務以資通訊系統蒐集、處理或利用中獎人個人資料者，應採行下列資訊安全措施：

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、非法或異常使用行爲之監控與因應機制。

2 前項第五款及第六款所定措施，應定期演練及檢討改善。

第 18 條

發行機構針對保有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之環境，應採取下列環境安全管理措施：

一、依據作業內容之不同，實施適宜之進出管制方式。

二、所屬人員妥善保管個人資料之儲存媒介物。

三、針對不同媒介物存在之環境，審酌建置適度之保護設備或技術。

第 19 條

1 發行機構應採行適當措施，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，以供必要時說明其所訂本計畫之執行情況。

2 發行機構於業務終止後，針對個人資料參酌下列措施爲之，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。

3 前二項之紀錄、軌跡資料及相關證據，應至少留存五年。

第 20 條

發行機構應訂定個人資料安全稽核機制，定期或不定期查察是否落實執行所訂之本計畫等相關事項。

第 21 條

發行機構應參酌執行業務現況、社會輿情、技術發展、法令變化等因素，檢視所訂本計畫是否合宜，必要時予以修正。

第 22 條

1 本辦法自發布後三個月施行。

2 中華民國一百十年七月二十八日修正發布之第六條，自發布日施行。