公益彩券發行機構個人資料檔案安全維護管理辦法

條文	說明
第一條　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。	本辦法之法源依據。
第二條　本辦法適用對象為財政部指定擔任公益彩券之發行機構（以下簡稱發行機構）。 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。 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。	鑑於公益彩券發行機構因執行業務需要，保有大量個人資料(如彩券經銷商、代理人、雇員、受託批購人、中獎人等)，爰將其列為受規範對象，以落實個人資料檔案之安全維護與管理。
第三條　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。 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。 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。	一、配合本法施行細則第十二條第二項第一款、第七款規定有關配置管理之人員、相當資源及宣導與訓練等事項，於第一項明定發行機構應配置相當人力、資源，以執行相關任務；另為利代表人善盡督導之責，第二項明定個人資料檔案安全維護管理組織應定期向代表人或經其授權之人員，以書面報告相關執行情況。 二、復為確認本計畫之訂定或修正核定單位，爰於第三項明定須經發行機構代表人或經其授權之人員核定，以利遵循，並避免事後產生爭議。
第四條　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。	配合本法施行細則第十二條第二項第二款規定有關界定個人資料範圍事項，明定發行機構應定期查核及界定個人資料之範圍，以利

	個人資料安全維護。
第五條　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。	配合本法施行細則第十二條第二項第三款規定有關個人資料風險評估及管理機制事項，明定發行機構應分析判斷於蒐集、處理及利用過程中，個人資料安全可能發生之風險，俾採行適當管控措施保護個人資料，以降低風險。
第六條　發行機構為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。 發行機構遇有個人資料安全事故者，應即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。 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。	一、配合本法施行細則第十二條第二項第四款規定有關事故之預防、通報及應變機制事項，明定發行機構應採取之因應措施，以降低或控制損害，並讓當事人瞭解相關狀況，使當事人亦能採取相關措施防止損害發生或擴大，此外，亦應研議預防機制，防杜事故發生。 二、另參酌「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」第六條第二項及第三項有關業者遇有危及正常營運或大量當事人權益之重大個資安全事故，其所研議之預防措施，應經公認認證資格之專家進行整體診斷之規定，於第三項規定之，以強化預防機制。
第七條　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，惟如認為具有特別管理之需要，仍得比照或訂定特別管理程序。	配合本法施行細則第十二條第二項第五款規定有關蒐集、處理及利用之內部管理程序事項，明定發行機構應依個人資料之屬性訂定管理程序，以利個人資料安全維護。
第八條　發行機構為遵守本法第八條及第	配合本法施行細則第十二條第二項第五款規

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。	定有關蒐集、處理及利用之內部管理程序事項，明定發行機構應遵循本法有關告知義務之方式，以利個人資料安全維護。
第九條　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。 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。	配合本法施行細則第十二條第二項第五款規定有關蒐集、處理及利用之內部管理程序事項，明定發行機構應遵循本法有關蒐集、處理及利用個人資料之特定目的及法定要件，以利個人資料安全維護。
第十條　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為適當之監督，並明確約定相關監督事項與方式。	配合本法施行細則第十二條第二項第五款規定有關蒐集、處理及利用之內部管理程序事項，明定發行機構應遵循本法施行細則有關委託他人蒐集、處理或利用個人資料所應負之監督責任，以利個人資料安全維護。
第十一條　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。	配合本法施行細則第十二條第二項第五款規定有關蒐集、處理及利用之內部管理程序事項，明定發行機構應遵循本法有關行銷規範，以利個人資料安全維護。
第十二條　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為限制國際傳輸之命令或處分，並應遵循之。	配合本法施行細則第十二條第二項第五款規定有關蒐集、處理及利用之內部管理程序事項，明定發行機構應遵循本法有關國際傳輸規範，以利個人資料安全維護。
第十三條　發行機構為提供資料當事人行使本法第三條所規定之權利，應採取下列方式為之： 一、確認是否為個人資料之本人，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	配合本法施行細則第十二條第二項第五款規定有關蒐集、處理及利用之內部管理程序事項，明定發行機構應遵循本法有關資料當事人行使權力之規範，以利個人資料安全維護。

知當事人。	
第十四條　發行機構為維護其所保有個人資料之正確性，應採取下列方式為之： 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。	配合本法施行細則第十二條第二項第五款規定有關蒐集、處理及利用之內部管理程序事項，明定發行機構應遵循本法有關資料正確性之規範，以利個人資料安全維護。
第十五條　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。	配合本法施行細則第十二條第二項第五款規定有關蒐集、處理及利用之內部管理程序事項，明定發行機構應遵循本法有關特定目的消失與期限屆滿之處理規範，以利個人資料安全維護。
第十六條　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。	配合本法施行細則第十二條第二項第六款規定，就人員管理事項，明定發行機構應採行之人員管理措施，以確保個人資料安全維護。
第十七條　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。	配合本法施行細則第十二條第二項第六款規定，就資料安全管理事項，明定發行機構應採行之資料安全管理措施，以確保個人資料安全維護。
第十八條　發行機構針對保有個人資料存	配合本法施行細則第十二條第二項第八款規

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。	定，就設備安全管理事項，明定發行機構應採行之環境與設備安全管理措施，以確保個人資料安全維護。
第十九條　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。 發行機構於業務終止後，針對個人資料參酌下列措施為之，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。 前二項之紀錄、軌跡資料及相關證據，應至少留存五年。	一、配合本法施行細則第十二條第二項第十款規定有關使用紀錄、軌跡資料及證據保存事項，明定發行機構應留存相關軌跡紀錄，以明確個人資料使用歷程情形，並避免爭議。 二、另按本法第三十條有關損害賠償請求權，應自損害發生時起五年內行使。為避免發生損害請求賠償時，相關紀錄已遭發行機構提前銷毀，爰明定應至少留存五年。
第二十條　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。	配合本法施行細則第十二條第二項第九款規定有關資料安全稽核機制事項，明定發行機構應訂定個人資料安全稽核機制，以利落實執行相關規範。
第二十一條　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。	配合本法施行細則第十二條第二項第十一款規定有關個人資料安全維護之整體持續改善事項，明定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，適時檢討修正本計畫，俾利持續改善個人資料安全維護運作機制。
第二十二條　本辦法自發布後三個月施行。	為利業者因應調適，給予三個月之緩衝期。