運動彩券業個人資料檔案安全維護計畫實施辦法總說明

個人資料保護法(以下簡稱本法)第二十七條規定「(第一項)非公務機關保有個人資料檔案者,應採行適當之安全措施,防止個人資料被竊取、竄改、毀損、滅失或洩漏。(第二項)中央目的事業主管機關得指定非公務機關訂定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。(第三項)前項計畫及處理方法之標準等相關事項之辦法,由中央目的事業主管機關定之。」,考量發行機構或受委託機構保有大量運動彩券經銷商、虛擬通路會員或辦理運動彩券經銷商遴選時申請者之個人資料檔案,為有效保護該等檔案,避免遭到竊取、竄改、毀損、滅失或洩漏,發行機構或受委託機構應就該檔案訂定個人資料檔案安全維護計畫(以下簡稱計畫),包括業務終止後對該檔案之適當處理方法。為使發行機構或受委託機構於訂定計畫時有所依循,爰訂定運動彩券業個人資料檔案安全維護計畫實施辦法(以下簡稱本辦法),其要點如下:

一、本辦法之法源依據。(第一條)

二、本辦法之主管機關。(第二條)

三、運動彩券業應訂定計畫及本辦法適用之對象。(第三條)

四、運動彩券業訂定計畫時,應訂定適當之安全維護措施。(第四條)

五、運動彩券業應完成計畫訂定之期程及報主管機關備查。(第五條)

六、運動彩券業應指定專責人員負責個人資料檔案安全維護之相關任務。(第六條)

七、運動彩券業所保有之個人資料,經定期檢視,應予刪除、銷毀或停止蒐集、處理及利用之情形。(第七條)

八、運動彩券業蒐集及傳輸個人資料時應符合之規定。(第八條)

九、運動彩券業應依已界定之個人資料範圍與蒐集、處理及利用流程,訂定適當管控措施。(第九條)

十、運動彩券業蒐集個人資料應遵守之告知義務。(第十條)

十一、運動彩券業利用個人資料行銷時,應提供當事人拒絕機制及應遵守事項。(第十一條)

十二、運動彩券業對於當事人行使本法第三條規定之權利,得採行之辦

理方式。（第十二條）

十三、運動彩券業應訂定應變機制及通報主管機關之義務。（第十三條）

十四、運動彩券業應設置必要之安全設備及採取必要之防護措施。（第十四條）

十五、運動彩券業應對其所屬人員採取之措施。（第十五條）

十六、運動彩券業提供電子商務服務系統時，應採取之資訊安全措施。（第十六條）

十七、運動彩券業應訂定個人資料檔案安全維護查核機制並納入其內部控制及稽核制度。（第十七條）

十八、運動彩券業應留存個人資料使用紀錄、自動化機器設備之軌跡資料。（第十八條）

十九、運動彩券業應定期或不定期對其所屬人員施以個人資料保護相關法令規定之教育訓練或宣導。（第十九條）

二十、運動彩券業業務終止後，對其保有之個人資料之處理方法及留存紀錄。（第二十條）

二十一、運動彩券業應檢視所定計畫之合宜性，以持續改進個人資料保護機制。（第二十一條）

運動彩券業個人資料檔案安全維護計畫實施辦法

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。	個人資料保護法(以下簡稱本法)第二十七條規定：「(第一項)非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。(第二項)中央目的事業主管機關得指定非公務機關訂定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。(第三項)前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。」，爰明定本辦法之法源依據。
第二條　本辦法之主管機關為教育部。	明定本辦法之主管機關。
第三條　運動彩券業應訂定個人資料檔案安全維護計畫（以下簡稱計畫），落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 前項所稱運動彩券業，指運動彩券發行條例第三條第二款、第三款所定發行機構及受委託機構。 第一項計畫，應包括運動彩券發行條例第三條第四款所定經銷商所保有個人資料檔案之安全維護事項；其訂定或修正，應經運動彩券業董事會決議或經其授權之經理部門核定。	一、第一項，明定運動彩券業應訂定個人資料檔案安全維護計畫（以下簡稱計畫），以建立相關管理機制並落實執行。 二、第二項，明定本辦法適用對象。 三、第三項，明定發行機構及受委託機構訂定之計畫內容，應包括經銷商所保有個人資料檔案之安全維護事項；另以本法及其施行細則並未規定計畫之訂定或修正，是否須經非公務機關董事會決議或經其授權之經理部門核定，為使計畫之訂定或修正有所遵循，爰予以明定。
第四條　運動彩券業訂定計畫時，應就其保有個人資料之性質及數量等事項，訂定適當之安全維護措施。	考量運動彩券發行機構及受委託機構保有個人資料之性質及數量不盡相同，另依本法施行細則第十二條第二項規定，所採行之安全措施與所欲達成之個人資料保護目的間，應符合比例原則，爰明定運動彩券業應就其保有個人資料之性質及數量等事項，訂定適當之安全維護措施。
第五條　運動彩券業應於本辦法發布施行之日起六個月內，完成計畫之訂	為使主管機關監督運動彩券業建立相關個人資料檔案安全維護管理機制，爰明

定，並報主管機關備查。	定運動彩券業應於本辦法發布施行之日起六個月內，完成計畫之訂定，並報主管機關備查。
第六條　運動彩券業應指定專責人員，負責規劃、訂定、修正、執行計畫及業務終止後個人資料處理方法等相關事項，並定期向負責人提出報告。	依本法施行細則第十二條第一項及第二項第一款規定，本法第二十七條第一項所稱適當之安全措施，指為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施，得包括配置管理之人員及相當資源，為有效訂定與執行計畫，爰明定運動彩券業應指定專責人員，負責個人資料檔案安全維護。
第七條　運動彩券業應確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查所保有之個人資料現況。 運動彩券業經定期檢視，發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或為其他停止蒐集、處理或利用等適當之處置。	一、依本法施行細則第十二條第二項第二款規定，適當之安全措施得就界定個人資料範圍相關事項加以規定，爰於第一項明定運動彩券業應依蒐集之特定目的，界定所蒐集、處理及利用個人資料之類別或範圍，並定期清查保有之個人資料現況。 二、第二項，明定運動彩券業就其保有之個人資料，經定期檢視，有應予刪除、銷毀或停止蒐集、處理及利用之情形時之處理方式。
第八條　運動彩券業於蒐集個人資料時，應檢視是否符合前條第一項所定之類別及範圍。 運動彩券業於傳輸個人資料時，應採取必要保護措施，避免洩漏。	一、第一項，明定運動彩券業於蒐集個人資料時，應配合檢視之內容。 二、為避免於傳輸個人資料時洩漏相關資料，爰於第二項明定運動彩券業應採取必要保護措施。
第九條　運動彩券業應依已界定個人資料之範圍與蒐集、處理及利用流程，分析評估可能發生之風險，訂定適當之管控措施。	明定運動彩券業應考量整體業務運作狀況，就已界定之個人資料之範圍與蒐集、處理及利用流程，分析評估可能發生之風險，並針對該可能發生之風險，採取必要之防範與管控措施，避免個人資料被竊取、竄改、洩漏、毀損或滅失。
第十條　運動彩券業於蒐集個人資料時，應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知	明定運動彩券業除有例外免告知之事由外，應依本法第八條及第九條規定，踐行告知之義務。

方式、內容及注意事項，要求所屬人員確實辦理。	
第十一條　運動彩券業利用個人資料行銷時，應明確告知當事人該運動彩券業之名稱及個人資料來源。 運動彩券業於首次利用個人資料行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用；當事人表示拒絕接受行銷者，應立即停止利用個人資料，並周知所屬人員。	一、第一項，明定運動彩券業利用個人資料行銷時，應明確告知當事人運動彩券業之名稱及個人資料來源。 二、運動彩券業利用個人資料行銷時，應依本法第二十條第二項及第三項規定辦理，爰於第二項明定運動彩券業應提供當事人表示拒絕接受行銷之方式及拒絕之效果。
第十二條　運動彩券業於當事人行使本法第三條規定之權利時，得採取下列方式辦理： 一、提供聯絡窗口及聯絡方式。 二、確認是否為資料當事人之本人，或經其委託。 三、有本法第十條但書、第十一條第二項但書或第三項但書得拒絕當事人行使權利之事由，一併附理由通知當事人。 四、告知是否酌收必要成本費用及其收費基準，並遵守本法第十三條處理期限規定。	明定運動彩券業對於當事人行使本法第三條規定之權利時，得依各款所定方式辦理。
第十三條　運動彩券業應訂定應變機制，在發生個人資料被竊取、洩漏、竄改或其他侵害事件時，迅速處理，以保護當事人之權益。 前項應變機制，應包括下列事項： 一、採取適當之措施，控制事件對當事人造成之損害。 二、查明事件發生原因及損害狀況，並以適當方式通知當事人。 三、研議改進措施，避免事件再度發生。 運動彩券業應自第一項事件發生之日起三日內，通報主管機關；並自處理結束之日起一個月內，將處理方式及結果，報主管機關備查。	一、依本法第十二條規定，非公務機關所持有之個人資料發生被竊取、洩漏、竄改或其他侵害事件者，應查明後以適當方式通知當事人，爰於第一項明定運動彩券業應訂定相關應變機制。 二、第二項，明定前項應變機制應包括事項，以保護當事人權益。 三、第三項，參考金融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規定，明定運動彩券業應自發生第一項所定事件之日起三日內，通報主管機關，並於規定期限內將處理方式及結果報主管機關備查。

第十四條　運動彩券業對所保有之個人資料檔案，應設置必要之安全設備及採取必要之防護措施。 前項安全設備或防護措施，應包括下列事項： 一、紙本資料檔案之安全保護設施及管理程序。 二、電子資料檔案存放之電腦或自動化機器相關設備，配置安全防護系統或加密機制。 三、訂定紙本資料之銷毀程序；電腦、自動化機器或其他儲存媒介物需報廢汰換或轉作其他用途時，應採取適當防範措施，避免洩漏個人資料。	一、為確保運動彩券業所保管之個人資料檔案不被竊取、竄改、毀損、滅失或洩漏，爰於第一項明定運動彩券業對所保有之個人資料，應設置必要之安全設備及採取必要之防護措施。 二、第二項，明定安全設備或防護措施之內涵。
第十五條　運動彩券業為確實保護個人資料之安全，應對其所屬人員採取下列措施： 一、依據業務作業需要，建立管理機制，設定所屬人員不同之權限，以控管其接觸個人資料之情形，並定期確認權限內容之適當性及必要性。 二、檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。 三、要求所屬人員妥善保管個人資料之儲存媒介物，並約定保管及保密義務。 四、所屬人員離職時取消其識別碼，並應要求將執行業務所持有之個人資料(包括紙本及儲存媒介物)辦理交接，不得攜離使用，並應簽訂保密切結書。	運動彩券業與其所屬人員，均應避免其保管或蒐集、處理及利用個人資料時，違反個人資料保護相關法令規定，致侵害當事人權益，爰明定運動彩券業應採取必要且適當之管理措施。
第十六條　運動彩券業提供電子商務服務系統時，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。	一、依運動彩券發行條例第十一條規定，運動彩券業得利用電話、網際網路及其他電訊設備銷售運動彩券，考量網際網路對於個人資料安

三、網際網路傳輸之安全加密機制。 四、應用系統於開發、上線、維護等各階段軟體驗證及確認程序。 五、個人資料檔案與資料庫之存取控制及保護監控措施。 六、防止外部網路入侵對策。 七、非法或異常使用行為之監控及因應機制。 前項所稱電子商務，指透過網際網路進行有關商品或服務之廣告、行銷、供應或訂購等各項商業交易活動。 第一項第六款及第七款所定措施，應定期演練及檢討改善。	全之潛在風險，需採行相關個人資料安全保護措施，包括系統使用者之身分確認、個人資料顯示之隱碼去識別化機制、網際網路傳輸之安全加密、系統正常運作之驗證與確認、系統中個人資料檔案及資料庫之存取控制與保護監控、防範外部網路入侵及其他非法或異常使用等，並將相關內容明定於計畫中，爰於第一項各款予以明定。 二、第二項，參考行政院所定電子商務消費者保護綱領，明定電子商務之定義。 三、為使運動彩券業提供之電子商務系統遭遇各類資安事件時，得以儘速恢復正常並控制損害，爰於第三項明定運動彩券業宜針對防範非法入侵或異常使用等應變措施定期進行演練及檢討改善。
第十七條　運動彩券業應訂定個人資料檔案安全維護查核機制，定期或不定期檢查計畫之執行情形，並將檢查結果向負責人提出報告。 執行前項查核之人員與第六條指定之專責人員，不得為同一人。 運動彩券業應將第一項查核機制，納入其內部控制及稽核項目中。	一、運動彩券業為確保個人資料維護安全措施發生效能，爰於第一項前段明定運動彩券業應訂定個人資料檔案安全維護查核機制，定期或不定期檢查計畫之執行情形；又依本法第五十條規定，對非公務機關之代表人，因該非公務機關依本法第四十七條至第四十九條規定受罰鍰處罰時，除能證明其已盡防止義務者外，應受同一額度罰鍰處罰，爰於同項後段明定運動彩券業應向負責人提出檢查結果報告，俾利負責人得據以監督計畫之執行事項，落實對個人資料之保護。 二、第二項，明定查核人員與負責規劃、訂定、修正及執行計畫之專責人員不得為同一人。 三、以個人資料檔案安全維護屬內部控制及稽核制度之重要一環，爰於第

	三項明定運動彩券業應將查核機制納入其內部控制及稽核項目中。
第十八條　運動彩券業應採行適當措施，留存個人資料使用紀錄、自動化機器設備之軌跡資料或其他相關之證據資料，以供必要時說明其所定計畫之執行情況。	運動彩券業為證明確實執行本計畫及執行方法，已盡防止個人資料遭侵害之義務，應採行適當措施並留存相關證據，以供日後發生問題時提供說明佐證，免除或減輕其法律責任，爰予以明定之。
第十九條　運動彩券業對於個人資料蒐集、處理及利用，應符合本法第十九條及第二十條規定。 運動彩券業應定期或不定期對其所屬人員施以教育訓練或認知宣導，使其明瞭個人資料保護相關法令規定、責任範圍、作業程序及應遵守之相關措施。	一、第一項，明定運動彩券業對個人資料之蒐集、處理及利用，應依本法第十九條及第二十條規定辦理。 二、為避免發生違反本法之情事，爰於第二項明定運動彩券業應定期對所屬人員施以教育訓練或認知宣導，使所屬人員充分明瞭個人資料保護相關法令及責任範圍。
第二十條　運動彩券業業務終止後，其保有之個人資料，應依下列方式處理並留存紀錄: 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、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。 前項紀錄應至少留存十年。	一、運動彩券業因發行權屆滿或其他原因終止運動彩券發行後，自不得再繼續使用其所保有之個人資料檔案，並應作妥善處置，爰於第一項明定運動彩券業銷毀、刪除、移轉或刪除、停止處理或利用個人資料過程中，應保存處理方式、地點、時間、執行人員、接受移轉資料之對象及合法移轉依據等資料，俾利日後舉證。 二、配合運動彩券管理辦法第二十五條規定「發行機構及受委託機構應蒐集處理運動彩券發行相關資料，並保存至其發行權屆滿後十年。」之年限規定，爰於第二項明定運動彩券業業務終止後，其保有之個人資料之銷毀、移轉或刪除、停止處理或利用之紀錄，至少留存十年。
第二十一條　運動彩券業應參酌計畫執行狀況、技術發展、法令依據修正等因素，檢視所定計畫是否合宜，必要時應予以修正。	明定運動彩券業應依實務運作情形，檢視或修正計畫。
第二十二條　本辦法自發布日施行。	明定本辦法施行日期。