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總說明

個人資料保護法第二十七條第二項、第三項規定，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；其相關事項之辦法，亦由中央目的事業主管機關定之。

依據「個人資料保護法非公務機關之中央目的事業主管機關」列表，金融監督管理委員會(以下簡稱本會)為存款機構、金融控股業、票券金融業、信用卡發卡業、證券金融業、人身保險業、財產保險業、再保險業、證券業及期貨業等之中央目的事業主管機關。考量此等業者保有大量且重要之個人資料檔案，其所負之安全維護責任應較一般行業為重，爰依上開規定之授權制定本辦法，要求該等非公務機關訂定個人資料檔案安全維護計畫及業務終止後個人資料處理方法(下稱本計畫及處理方法)，以加強管理、確保個人資料之安全維護。

本辦法共計五章、十六條，其訂定要點如下：

一、應適用本辦法之非公務機關，包括各類金融服務業及本會主管之財團法人。(第二條)

二、非公務機關應依其業務規模及特性，衡酌經營資源之合理分配，配置管理人員及相當資源，以規劃、訂定、修正與執行本計畫及處理方法，並提交其經營管理階層核定或簽署。(第三條)

三、非公務機關應依個人資料保護相關法令，定期查核確認所保有之個人資料現況，界定其納入本計畫及處理方法之範圍，並依所界定之結果，評估可能產生之個人資料風險，訂定適當之管理機制。(第四條及第五條)

四、為因應個人資料安全事故，非公務機關應於本計畫及處理方法中，訂定相關應變、通報、預防及強化機制。(第六條)

五、非公務機關應於本計畫及處理方法，訂定各類個人資料管理程序，包括：自行或委託從事個人資料蒐集、處理、利用、行銷、國際傳輸、刪除等之內部管理程序，及當事人行使權利之相關事

項等。（第八條）

六、非公務機關應於本計畫及處理方法中，訂定資料安全、人員及設備安全之相關管理措施；其利用網際網路提供電子商務服務系統者，並應採取相關資訊安全維護措施。（第九條至第十二條）

七、非公務機關應於本計畫及處理方法中，訂定個人資料之安全稽核、紀錄保存及持續改善機制，並明定其軌跡資料、相關證據及紀錄，應至少留存五年。（第十三條至第十五條）

八、本辦法自發布日施行。（第十六條）