6.4.5 隱私權保護

個資保護政策與組織

國泰金控重視並致力落實客戶隱私權及個資保護，國泰金控及主要子公司—國泰人壽保險、國泰世華銀行、國泰產險及國泰證券皆已制定「個人資料管理政策」與「個人資料檔案安全維護計畫暨業務終止後個人資料處理方法」並於官網公告以作爲對個人資料保護相關法令及良善管理承諾之遵循。本公司嚴格要求全體同仁及廠商應遵循個資保護相關要求，共同致力於個資安全維護，以保障個資所有人之權益。

國泰金控將個資保護納入至風險管理架構，設置「個人資料管理委員會」，由總經理擔任主任委員，督導與管理國泰個人資料管理機制落實與風險管控情形。由風險管理處擔任個資管理單位，依委員會之決議，負責規劃、監督執行及檢討改善集團之個資管理事項。

國泰金控設有直屬董事會之內部稽核單位，負責督導與執行公司及各子公司之稽核業務。每半年至少進行一次專案業務查核，範疇涵蓋財務、風險管理、法令遵循及個資保護等領域；每年至少辦理一次內部控制自行查核，並由稽核單位覆核各單位之檢查情況，確保員工全面落實相關管控要求。

客戶個資管理機制

國泰金控及主要子公司依據個人資料保護法相關法令，及個資生命週期（蒐集、處理及利用）進行個人資料管控。在蒐集個資前，明確告知客戶蒐集目的、應用及分享對象，並確保不逾越特定目的之必要範圍，於客戶同意後才會將特定的個人資料提供給合作供應產品及服務的第三方進行相關服務處理；在個人資料保存方面，除非法律或契約另有規定，會於蒐集目的消失或期限屆滿時，刪除或停止處理及利用個人資料，並保留相關軌跡資料或證據至少五年。

在個資防護方面，包括存取權限控管、防火牆、SSL 加密技術、OTP 身分驗證、登入行為偵測、浮水印警示、建立資料外洩防護（Data Loss Prevention，DLP）偵測與管理機制，及建立端點防護措施等。

管理機制與國際接軌

為強化自身之個資管理機制與因應歐盟一般資料保護規則（GDPR）之遵循，國泰金控及主要子公司皆已導入並通過「BS10012：2017 個人資料管理系統」與「ISO 27001 資訊安全管理系統」國際標準驗證，透過國際管理制度 P-D-C-A（Plan-Do-Check-Action）管理循環，及每年第三方專業外部驗證單位查核審視，確保個資保護流程與管控措施、廠商管理等面向之妥適性，並符合個資相關法令要求，持續完善管理機制。

客戶權利行使

國泰金控及主要子公司皆訂有「個人資料當事人權利行使相關管理辦法」並設有申訴與權利行使受理窗口與管道，提供客戶與員工提出相關需求。相關客戶權益保障已於國泰金控官網的「個人資料保護之法定告知事項」、「隱私權保護聲明」及「顧客資料保密措施」中明確公告，並將配合法令變動與因應最新技術隨時更新，同時亦提供服務諮詢專線與留言專區予客戶聯繫與反應。

完善的個資教育訓練

為使同仁明瞭個人資料相關法令之要求、所屬人員之責任範圍與個人資料保護相關之機制、程序及措施，國泰金控暨各子公司每年定期舉辦全體員工個人資料保護認知宣導及教育訓練，2025 年國泰金控及主要子公司之個資教育訓練完訓率皆達 100%。

另針對個人資料保護規定之違反行為，除個人資料保護法已有罰則外，國泰金控亦於「個人資料管理規則」中明定員工若違反規定，致使公司或客戶權益受損，將移送人事管理單位議處，展現公司對個資保護及客戶隱私之決心與零容忍態度。

註：上述完訓率係扣除因業務特性與人員差勤規劃（臨時外派、育嬰假、產假等）同仁計算。

侵害事件管理與演練

個資侵害事件管理，於事件通報、處理上，國泰金控及主要子公司建置「個人資料侵害事件管理辦法」及相關緊急應變程序，並設置跨部門「緊急應變小組」，以降低個資侵害事件發生時造成公司之衝擊，盡可能減少對當事人之損害，透過定期擬真情境演練，驗證內部作業程序之有效性，及識別個資保護措施不足之處，持續精進相關個資保護措施。

2025 年辦理跨部門個資侵害擬真演練，就雲端資料庫個資侵害事件管理流程進行檢視，以利即時應變與降低外洩損害。

個資保護事件

國泰金控及主要子公司謹慎妥善運用客戶資料，2025 年度統計資訊外洩案件共 20 件，資訊外洩案件與個資相關的占比為 100%，因上述事件而受影響的顧客數為 887 位，上述案件大多屬於客戶藉由管道申訴案件，經釐清後，主要為資訊處理疏漏及資料寄送對象錯置之個案事件，後續皆持續與當事人聯繫溝通，冀取得諒解並妥善處理。國泰金控將持續推動員工教育訓練及加強宣導作業，使所屬人員充分了解個資保護之重要性，並將持續強化及監控客戶個人資料之使用，精進相關保護措施，及監督第三方合作單位妥善管理客戶資料，以減少個資外洩事件情事之發生。