

元大金融控股股份有限公司及子公司個人資料保護指引

114年5月13日總經理核准公布

115年1月16日總經理修正公布

為確保本公司及子公司個人資料之蒐集、處理及利用均妥善管理，並加強個人資料之安全維護，本公司依據《個人資料保護法》、《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》及主管機關相關法令規範，業訂定《元大金融控股股份有限公司個人資料保護政策》（下稱《個人資料保護政策》）、《元大金融控股股份有限公司個人資料管理辦法》（下稱《個人資料管理辦法》）等規章，以建立個人資料保護制度並於各項業務落實執行，茲揭示本公司及子公司之個人資料保護管理措施如下：

一、《個人資料保護政策》適用範圍包括本公司與子公司及各項業務。

（一）本公司應制定個人資料之蒐集、處理、利用以及安全維護管理制度。

（二）子公司應依《個人資料保護政策》之精神，建立與其業務規模及複雜程度相符之個人資料保護管理制度，以確保個人資料之蒐集、處理及利用符合法令規定。

（三）依據《個人資料管理辦法》，本公司應就個人資料管理制度之實行與運作、個人資料安全管理原則等訂定相關規範，包括但不限於所有參與個人資料蒐集、處理、利用、傳輸、保存與銷毀等作業之人員均須遵守規定。

二、本公司應明定個人資料最小化原則、提供第三方個資之限制與個人資料之保存及銷毀規定。

（一）蒐集、處理及利用之個人資料應符合最小化原則，並應確認僅蒐集聲明範圍內執行業務所需之個人資料、處理及利用時應僅使用所需之最少量個人資料，另應確認不處理與特定目的範圍無關或不必要之個人資料。

（二）個人資料之蒐集，應有特定目的並符合相關法令，除依《個人資料保護法》相關規定辦理外，本公司承諾不向第三方蒐集非由當事人提供之個人資料。

（三）個人資料之處理及利用應於原告知事項或當事人原始同意之範圍內為之，並不得向第三方提供(provide)、出借(rent)或銷售(sell)個人資料。如欲進行同意範圍(完成交易或服務之目的)外之處理或利用，應另行依相關法令規定取得當事人同意。

（四）個人資料之保存應制定保存期限，如特定目的消失或保存期限屆滿，應採取不同方式銷毀，並確實執行安全控管措施。

三、本公司應明定個人資料之存取控制及保護措施。

（一）「個人資料處理、利用及傳遞作業之安全防護措施」：個資文件、檔案或媒體之處理或利用環境應有進出管制；非經授權人員調閱個資文件或檔案時，應有申請及核准程序；個人資料之傳遞需進行適當之加密措施。

- (二)「個人資料之安全控管措施」：人員進出集中保存個人資料之庫房或檔案櫃，須有實體存取控管措施，並留存進出調閱紀錄；經合法授與之存取權限，僅得在合法及符合業務目的下被存取。
- (三)本公司與各子公司間應採用區域虛擬網路系統，以分層管理個人資料；並應採用先進之防火牆系統，防止未經授權者入侵。
- 四、本公司應設立「個人資料保護小組」，以有效落實及整合個人資料保護相關事宜。
- (一)依據《個人資料管理辦法》，本公司應設立個資保護小組，並由總經理指定副總經理級以上主管擔任召集人及副召集人，及由各部室指派代表擔任小組成員，並視業務執行情形召開會議討論個資保護事宜。
- (二)個資保護小組每年至少進行一次個人資料保護管理審查，審查結果併同年度法令遵循制度執行情形提報董事會。
- 五、本公司應每年辦理個人資料風險評估，以有效管理業務上之個人資料風險。
- (一)本公司應依評估結果訂定控管措施，評估結果及相關分析均提報個資保護小組會議。
- (二)本公司若發生個人資料安全或外洩事件，除依規定程序通報作業風險事件外，涉及資訊面風險者，應依資訊安全風險相關規定辦理，並對於發生個資安全事件之原因，提供預防或改善建議。
- (三)本公司應將個人資料保護列入內部稽核查核項目及定期每年舉辦之教育訓練課程，以提升員工對於個人資料保護之認知。
- 六、本公司及子公司應訂有客戶資料保密措施，並應建立客戶就其個人資料行使法定權利之機制，以保障當事人之隱私及權利。
- (一)本公司及子公司已訂定並於官網揭露《元大金融控股股份有限公司暨子公司客戶資料保密措施》，明示本公司之子公司除該保密措施所定情形或經客戶書面同意外，不會向第三人揭露客戶個人資料。
- (二)本公司及子公司已於官網公告《隱私權保護聲明》，說明客戶得依法令或各公司之規定，請求查詢、閱覽、補充、更正及刪除個人資料。
- 七、本指引經總經理核准後公布於本公司網站，修正時亦同。