合作金庫金融控股股份有限公司個人資料保護管理政策

112 年 5 月 22 日第 4 屆第 35 次董事會審議通過

第 一 條 （目的）

合作金庫金融控股股份有限公司(以下稱本公司)為落實個人資料與隱私權保護之目的，並遵循個人資料保護相關法令之規範，以保障個人資料當事人權利，特訂定本政策。

第 二 條 （管理目標）

本政策之管理目標如下：

一、確保本公司及子公司各項業務之執行符合個人資料保護之各項法令規定、客戶契約及其他相關規範要求。

二、維護個人資料當事人之合法權益。

三、應於合法之組織營運、業務下，以合理安全之方式，於特定目的必要範圍內，蒐集、處理及利用個人資料。

四、提供個人資料檔案適當之安全措施，確保本公司及子公司對持有之個人資料已盡善良管理人之注意義務。

第 三 條 （適用對象）

本政策適用對象包括本公司、子公司與受本公司及子公司委託蒐集、處理或利用個人資料之供應商。

子公司應參酌本政策，考量其業務規模及性質，制定個人資料保護管理組織及制度，並將上開制度納入該公司內部控制及稽核項目，另應依本政策督導其轄下子公司，以落實執行個人資料保護管理。

第 四 條 （管理組織與運作）

本公司應設置個人資料保護管理組織並配置相當資源，督導本公司及子公司之個人資料保護管理，並指派專責單位或人員負責規劃、協調並建立個人資料保護管理規定及制度。

本公司應將個人資料保護納入公司之風險管理監督，並將相關機制列入內部控制及稽核項目，以確保本政策及相關規範之落實執行。

第 五 條　（個人資料蒐集、處理及利用原則）

個人資料蒐集、處理及利用原則如下：

一、應識別所處理之個人資料，並界定個人資料範圍，以建立個人資料檔案。

二、基於合法之特定目的，在必要之範圍內蒐集、處理及利用個人資料，並於必要時進行更新以維護個人資料之正確性及完整性，並確保個人資料之安全。

三、應明確告知當事人法定應行告知事項。

四、尊重當事人對其個人資料權利之行使，包含查詢或請求閱覽、請求製給複製本、請求補充或更正、停止蒐集、處理或利用及請求刪除等，並提供適當之協助。

五、國際傳輸個人資料應符合法令或主管機關相關規範，且於適當充分保護下方可進行。

六、當個人資料應用於個人資料保護法所允許之例外情形時，應確保其適當性與合法性。

七、建立與實施個人資料保護管理制度，落實個人資料保護管理政策。

八、於個人資料保護管理制度運行中，明確界定員工之責任與義務。

九、適當留存個人資料蒐集、處理與利用之軌跡紀錄。

十、建立個人資料安全事故應變及預防程序，並於個人資料侵害事件發生時依規處理並通報。

十一、委託蒐集、處理及利用個人資料者，應為適當之監督，並於委託契約或相關文件中，明確約定其內容。

十二、應採取適當之個人資料安全管理措施(如：防火牆)，以防止遭到不法入侵及避免資料遭到非法存取。

十三、若個人資料當事人應適用歐盟一般資料保護規則（General Data Protection Regulation，GDPR）時，應建立相關規範確保合規，並依其規定告知當事人法定應行告知事項及提供

當事人得行使之權利（如：限制處理或利用方式、資料攜出權）。

第 六 條　（風險評估與定期稽核）

本公司應依業務作業流程產生之個人資料檔案，評估可能面臨之風險，並根據風險評估之結果，訂定適當之控制措施。

本公司應定期辦理內部稽核，查核個人資料保護管理制度及執行之有效性；子公司依主管機關要求，應委託外部機構辦理查核。

本公司對於內外部查核結果，應予改善以維護個人資料保護管理制度之運作。

第 七 條　（零容忍政策）

本公司或子公司所屬人員如違反個人資料保護相關法令或內部規範，應視情節輕重依相關規定懲處或追究法律責任。

供應商及其所屬人員如違反個人資料保護相關法令或契約有關個人資料保護之約定，致本公司或子公司受有損害時，應負損害賠償責任。

第 八 條　（檢視與更新）

本公司應適時檢視本政策，以反映政府法令、個人資料管理技術、主管機關要求及公司業務等最新發展狀況，確保個人資料保護管理實務作業之合規及有效性。

第 九 條　（附則）

本政策如有未盡事宜，悉依個人資料保護相關法令、歐盟一般資料保護規則與本公司及子公司相關規定辦理。

第 十 條　（施行）

本政策經董事會通過後施行，修正時亦同。