王道商業銀行個人資料管理政策

經2017.4.28第六屆第27次董事會核准實施

經2021.2.24第八屆第6次董事會核准實施

經2023.12.27第九屆第5次董事會核准實施

經2024.06.27第九屆第10次董事會核准實施

目錄

一、 目的

王道商業銀行(以下簡稱本行)為落實個人資料保護及管理，並遵循《個人資料保護法》之相關要求及保障個人資料當事人之權利，降低任何個人資料受侵害之事件所可能帶來的衝擊，特訂定本行個人資料管理政策（以下簡稱本政策）。

二、 範圍

本政策敘述本行之個人資料管理體系之架構與建置方法，闡明本行同仁應遵循的個人資料保護政策，以及在個人資料管理的工作規劃、實踐與持續改進過程中所應扮演的角色與權責。

本行所有人員均屬適用本政策的涵蓋對象。本政策所定義之個人資料範圍與類別，係以各單位於符合本行營業登記項目或法令准許之業務及其相關延伸業務、行政管理目的下，直接或間接取得實際所蒐集之個人資料為準。

三、 名詞定義

(一) 個人資料管理體系

以營運風險導向為基礎，用以建立、實作、運作、監視、審查、維持及改進個人資料管理。

(二) 所有人員

涵蓋本行所有員工、臨時雇員、承包商(委託第三方服務廠商)。

(三) 有效性量測指標

定義如何衡量所選擇的控制措施之有效性，以達成本行個人資料管理目標。

(四) 個人資料侵害事件

未經個人資料當事人授權使用或不當蒐集、存取及揭露個人資料而超乎預期使用狀況皆屬之。

(五) 管理階層

本行個人資料管理之管理階層，包含董事長、總經理、法令遵循主管、稽核部主管及各部門主管等。

四、 權責

本行所有人員，皆應瞭解並確實遵守本政策。

五、 內容

以下內容條列應遵循之事項：

(一) 個人資料管理目標

本行個人資料管理目標如下：

1.符合我國個人資料保護之法令法規、主管機關命令以及客戶契約或專業職責等要求；

2.維護個人資料當事人之人格權，提供其個人資料的完全自主權；

3.對個人資料之蒐集、處理及利用過程，於特定目的範圍內以誠實信用方法為之，並應與蒐集之目的具有正當合理之關聯；

4.承諾實施特定且具代表性的資料保護標準和保障措施以確保本行得以盡良善管理之注意義務；

5.訂定個人資料保護之可接受的風險程度與因應措施；

6.承諾當個資事件發生導致利害關係人權益受損時(包括但不限於資料外洩)，將及時通知受影響的客戶進行適當地回應與處理，並於相關政策變更生效前提前通知客戶。

(二) 個人資料管理政策

1. 本行個人資料管理政策如下：

(1)遵守我國個人資料保護相關之法令規定。

(2)本行僅就基於合法、正當合理的特定目的，在確實必要的範圍內蒐集個人資料；

(3)基於合法、正當合理的特定目的蒐集及處理最少的必要個人資料；

(4)本行應清楚告知當事人，其個人資料將如何被使用；

(5)確保直接向未成年人蒐集資料時受到特別保護；

(6)已蒐集的客戶資料應作適當且相關的處理；

(7)公平合法地處理個人資料；

(8)維持一份本行處理的個人資料類別清單；

(9)確保個人資料的正確性，並於必要時進行更新；

(10)已蒐集的個人資料將會依法或在合法的特定目的下保存；

(11)尊重當事人對其個人資料所能行使之權利，包含查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理或利用及請求刪除等；

(12)以適當安全之水準技術保護其所蒐集、處理、利用之個人資料，確保所有個人資料的安全；

(13)只有在確實並受適當充分保護的狀況下，本行才會將個人資料進行國際傳輸；

(14)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；

(15)建立與實施個人資料管理制度並持續維運，讓個人資料保護政策落實，以確保個人資料檔案之安全；

(16)鑑別內外部利害關係者及其參與個人資料管理制度治理與運作的程度；

(17)於個人資料管理制度運行中，明確界定員工之責任與義務；

(18)規劃緊急應變程序以處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故；

(19)如有委託蒐集、處理及利用個人資料時，妥善監督受託機關；

(20)設置聯絡窗口，供當事人行使關於個人資料之權利或提出相關之申訴與諮詢；

(21)應維護個人資料的處理紀錄。

2. 為宣達本政策，亦以「個人資料管理政策聲明」進行公告。

(三) 個人資料管理組織

本行為落實個人資料之保護及管理，將明定個人資料管理體系內相關人員之權限及責任，以確實推行及監督個人資料保護機制。

(四) 個人資料管理體系

本行個人資料管理體系採用「Plan-Do-Check-Act (PDCA)」之循環運作模式，說明如下：

1.規劃與建立(Plan)

依據本行整體策略與目標，藉由成立個人資料管理組織，控制潛在之威脅及漏洞，規劃風險評估與安全控管機制，以建立個人資料管理體系。

2.實施與運作(Do)

依據評估規劃之結果，建立或修正應有之個人資料管控機制。

3.監督與查核(Check)

監督個人資料管理體系各項作業之落實執行，並查核其有效性。本政策將與本行現行稽核制度並行，定期實施個人資料內部稽核，以確保個人資料管理之落實。

4.維護與改進(Act)

根據監督查核之結果與建議，執行矯正與預防措施，改善並執行應有之控管機制，以持續維護個人資料管理體系之運作。

(五) 有效性量測指標

1.為確保個人資料管理目標之達成度，本行將制訂有效性量測指標。

2.有效性量測指標應衡量所選擇控制措施之有效性，並依評估控制措施及衡量時機，以產生可比較與可再製的結果。

(六) 管理階層責任

對於本行個人資料管理體系之規劃、建立、實施、運作、監督、查核、維護與改進各項作業，管理階層應訂定並遵循下列事項：

1.管理階層承諾

管理階層應確保完成下列工作，表示對個人資料管理發展及增進的充分支持：

(1) 核准個人資料管理目標與政策；

(2) 確認有效性量測指標之建立；

(3) 訂定個人資料管理之角色與職責；

(4) 提供個人資料管理體系各項作業所需之資源；

(5) 決定風險可接受水準；

(6) 執行個人資料管理體系之管理審查作業；

(7) 依本政策要求督導建立和實行個人資料管理體系。

2. 組織文化的深植

(1) 確認所有人員均具備工作所需相關職能；

(2) 評估職能訓練與相關措施之有效性；

(3) 建立並維護教育訓練、技能、經驗與資格之相關紀錄；

(4) 宣導遵守本政策與法令規章、達成有效性量測指標及持續改善之重要性。

(七) 個人資料管理體系查核

管理階層應確保定期或不定期進行個人資料管理體系的評估或查核作業，以檢討管制目標、管控措施與程序是否合乎相關標準、法令規章或個人資料管理需求，並依預期規劃有效執行與維持，以持續增進個人資料管理體系的有效性。

(八) 個人資料管理體系管理階層審查

管理階層應定期或在發生重大變化時執行管理審查，以確保個人資料管理體系運作之適切性、充足性及有效性。

(九) 個人資料管理體系之持續改進

組織應藉由稽核結果、矯正及預防措施及管理階層審查，以持續改進個人資料管理體系之有效性。

(十) 政策指導與覆核

本政策應每年至少評估一次，以反映政府法令、資訊技術及本行業務等最新發展狀況，確保個人資料管理實務作業之有效性。

(十一) 政策與法令之遵循

所有人員均應遵循本政策，違反者須依本行相關規定予以處分。如涉有相關民事賠償、刑事責任、行政裁罰者，本行得終止其僱傭關係並衡酌情節追訴其法律責任。員工對於本行之個人資料保護義務於雙方終止僱傭關係後仍繼續有效。

六、 表單/附件

為落實個人資料保護及管理，應訂定並發布「個人資料管理政策聲明」。

七、 核准權限

本政策由董事會核定後實施，修改時亦同。

本政策所涉及之相關作業或稽查，授權個人資料管理委員會或依本行分層負責表所訂權限另訂有關規定規範之。