

富邦金融控股股份有限公司暨子公司
個人資料保護管理政策

Fubon Financial Holding Co., Ltd. and Subsidiaries
Personal Information Protection Policy

文件編號	:	FHC-O-PIM-1-20230413
核准日期	:	2023/04/13
生效日期	:	2023/04/14
權責單位	:	風險控管處作業風險暨綜合規劃部
版序	:	第 7 版
Document No.	:	FHC-O-PIM-1-20230413
Approval Date	:	2023/04/13
Effective Date	:	2023/04/14
Responsible Unit	:	Risk Management Division, Operational Risk & Planning Department
Version	:	Version 7

第一條 訂立目的

為加強富邦金融控股股份有限公司（下稱「本公司」）及本公司營業執照所載之子公司（下稱「子公司」）對於個人資料之保護與管理，降低營運風險，及保護個人資料當事人權利，特訂定「富邦金融控股股份有限公司暨子公司個人資料保護管理政策」（下稱「本政策」），俾利遵循。

Article 1 Purpose of Establishment

The Fubon Financial Holding Co., Ltd. and Subsidiaries Personal Information Protection Policy (hereinafter “the Policy”) has been established to strengthen the protection and management of personal information by Fubon Financial Holding Co., Ltd. (hereinafter “the Company”) and the subsidiaries listed on the Company’s business license (hereinafter “subsidiaries”), lower operational risk, safeguard the rights of those the information belongs to and ensure compliance.

第二條 適用範圍

本政策適用於本公司及子公司。

子公司倘因其業務規模、性質或其應適用之相關法令等因素擬另訂相關規範者，應事前會簽本公司風險控管處。

子公司應依本政策原則督導其轄下子公司。

Article 2 Applicable Scope

The Policy applies to the Company and its subsidiaries.

If a subsidiary wants to separately establish its own related guidelines because of the size or nature of its business or because of related laws or regulations that it must comply with, it should first submit its proposed plan for approval to the Company’s Risk Management Division.

Subsidiaries shall oversee the activities of their subsidiaries based on the principles of the Policy.

第三條 個人資料保護管理之目標

個人資料保護管理目標如下：

- 一、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。

Article 3 Objectives of Personal Information Protection Management

The objectives of protecting and managing personal information are as follows:

1. To comply with laws and regulations on personal information protection, customer contracts and the requirements of related standards and rules;
2. To maintain the legitimate rights and interests of the party of personal information.

第四條 定義及說明**一、 個人資料：**

指依照中華民國個人資料保護法及其施行細則及相關業法規定所定義之個人之資料。

二、 個人資料檔案：

指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

三、 蒐集：

指以任何方式取得個人資料。

四、 處理：

指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

五、 利用：

指將蒐集之個人資料為處理以外之使用。

六、 國際傳輸：

指將個人資料作跨國（境）之處理或利用。

七、 個人資料保護管理體系：

指建立、運作、監督、查核、維護及改善個人資料保護管理之架構及制度。

八、 個人資料侵害事件：

未經個人資料當事人授權使用或不法蒐集、處理、利用個人資料或其他侵害當事人權利之狀況。

Article 4 Definitions

1. Personal information: refers to the personal information as defined in the Republic of China Personal Information Protection Act, Enforcement Rules of the Personal Information Protection Act, and relevant industry

laws and regulations.

2. Personal information file: a collection of personal information built to allow information retrieval and management by automatic or non-automatic measures.

3. Collection: collecting personal information in any form and way.

4. Processing: to record, input, store, edit, correct, duplicate, retrieve, delete, output, connect or internally transmit information for the purpose of establishing or using a personal information file.

5. Usage: all methods of personal information use other than processing.

6. International transmission: The cross-border processing or use of personal information.

7. Personal information protection management system: the framework and system used to develop, run, oversee, check, maintain and improve personal information protection management.

8. Personal information infringement cases: using personal information without authorization of the party concerned or illegally collecting, processing and using personal information or otherwise infringing on the rights of the party concerned.

第五條 個人資料保護管理組織與職責

- 一、 建立個人資料保護管理組織，並將個人資料保護管理體系之運行納入公司管理階層之監督管理。
- 二、 指派專責單位負責督導、協調、監控個人資料保護相關事宜。
- 三、 負責蒐集、處理、利用及保有個人資料之權責單位應依個人資料保護法相關規範執行個人資料保護。

Article 5 **Personal Information Protection Management Organization and Responsibilities**

1. A personal information protection management organization shall be built and the operations of the personal information protection management system shall be incorporated into the oversight and management responsibilities of the company's management.

2. A dedicated unit shall be assigned to take responsibility for guiding, coordinating and monitoring all matters related to personal information protection.

3. Dedicated units responsible for collecting, processing, using and keeping personal information shall execute their duties according to provisions in the Personal Information Protection Act.

第六條 個人資料蒐集、處理及利用原則

- 一、應識別所處理之個人資料，並界定個人資料範圍；
- 二、基於合法的特定目的，在必要的範圍內蒐集、處理及利用個人資料，於必要時進行更新以維護個人資料之正確性與完整性，並確保個人資料之安全；
- 三、應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，不得預先拋棄或以特約限制；
- 五、國際傳輸個人資料須符合主管機關相關規範，且在適當的保護下，方可進行國際傳輸。
- 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，應確保其適用性與合法性；
- 七、建立與實施個人資料保護管理體系，落實個人資料保護管理政策；
- 八、於個人資料保護管理體系運行中，明確界定員工之責任與義務；
- 九、當發生個人資料侵害事件時，應儘速依「個人資料保護法」、「富邦金融控股股份有限公司暨子公司作業風險呈報及管理辦法」及公司相關規範辦理及通報。若衍生媒體事件，應依「富邦金融控股股份有限公司暨子公司媒體危機處理準則」辦理；
- 十、受委託蒐集、處理及利用個人資料者，於個人資料保護法之適用範圍，視同委託機關。委託機構應妥善監督受委託機構，明訂受委託機構資訊安全責任及保密規定，並納入契約，要求受委託機構遵守，並定期予以查核。
- 十一、確保直接向未成年人蒐集的個人資料於利用、處理時，受到特別保護；
- 十二、應識別內、外部關注方，以及其對本公司個人資料保護治理之要求。

Article 6 Personal Information Collection, Processing and Usage Principles

1. Any personal information being processed should be identified and the information's scope should be defined;

2. Personal information should be collected, processed and used within the necessary scope for specific, lawful purposes and can be updated when necessary to make sure the information remains accurate and complete and see that it remains secure;
3. The party concerned should be notified of matters that the law requires to be disclosed;
4. The rights that parties can exercise related to their personal information should be respected, including inquiries or requests to review their personal information, requests to make copies of it, requests to supplement or correct it, requests to discontinue the collection, processing or usage of it, and requests to delete it. Those rights cannot be waived in advance or restricted by a special agreement;
5. The international transmission of personal information can only be done if it is in compliance with regulations set by the competent authorities and with appropriate protection;
6. When personal information is being used based on exceptions allowed under the Personal Information Protection Act, the usage of the information must be legitimate and legal;
7. A personal information protection management system should be devised and put in place to carry out the personal information protection policy;
8. The responsibilities and obligations of employees involved in the operations of the personal information protection management system should be clearly defined;
9. When there is an infringement of an individual's personal information, the case should be handled and reported as quickly as possible based on the "Personal Information Protection Act," "Fubon Financial Holding Co., Ltd. and Subsidiary Operational Risk Reporting and Management Guidelines," and other company rules. If the case leads to a media crisis, it should be handled based on the "Fubon Financial Holding Co., Ltd. and Subsidiary Principles for Media Crisis Management";
10. Those authorized to collect, process and use personal information are considered as a "commissioning agency" within the scope of the "Personal Information Protection Act." The commissioning agency should oversee other organizations or individuals it contracts and must meet the information security responsibilities and confidentiality regulations that are clearly stipulated for commissioning agencies. These obligations should be written into contracts, the contracted party should be asked to comply with them, and they should be reviewed on a regular basis.

11. Ensure that personal information collected directly from minors is specially protected during usage and processing;
12. Should identify internal and external interested parties and their requirements for the protection and governance of personal information of the Company.

第七條 個人資料保護管理體系之運作

本公司保有個人資料檔案者，應採取安全維護措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。個人資料保護管理體系運作之架構以「計畫-執行-檢查-行動」為基礎，在日常管理與營運上，落實資訊安全及個人資料保護法相關的規定：

- 一、計畫：建立個人資料保護管理組織架構、政策、目標及相關辦法、程序，並定期檢視而適時修正。
- 二、執行：實施個人資料保護管理制度，包括執行流程盤點、個人資料流分析、建立個人資料檔案清冊、執行個資管理風險評估，以辨識潛在之風險及漏洞，並據以建立或修訂個人資料保護管理相關規範及控管機制。
- 三、檢查：依據個人資料保護管理政策、辦法、程序及控管機制，檢查個人資料保護管理各項作業執行之情形，並提出改善建議。
- 四、行動：依據檢查的結果與建議，執行矯正與預防措施，以持續改善個人資料保護管理體系。
- 五、本公司個人資料管理單位或人員每年定期提出相關自我評估報告，使管理階層定期瞭解、掌握個人資料安全維護情形。
- 六、自我評估報告授權由總經理核定，並留存相關文件紀錄。

Article 7 **The Operation of the Personal Information Protection Management System**

Those in the company who keep personal information files should adopt security and maintenance measures to prevent personal information from being stolen, altered, damaged, destroyed or leaked. The operational framework of the personal information protection management system is based on the PDCA (plan-do-check-act) cycle and implements information security and “Personal Information Protection Act” provisions in the company’s daily management and operations:

1. Plan: Develop a personal information protection management organizational framework, policy, objectives and related guidelines and procedures, and review and adjust them when appropriate on a regular basis.
2. Do: Put in place a personal information protection management system that includes taking inventory of processes, analyzing personal information flows, developing a list of personal information files, and conducting information management risk assessments to identify hidden risks and gaps; then, based on the findings, set up or adjust information management rules and control mechanisms.
3. Check: Check how effectively the personal information protection system is being implemented based on personal information protection policies, guidelines, processes and control mechanisms and make suggestions for improvement.
4. Act: Based on the review's findings and suggestions, carry out corrective and preventive measures that will continue to improve the personal information protection management system.
5. The company's personal information management unit or personnel must submit an annual self-assessment report to keep management up to date on the security and maintenance of personal information.
6. The president of the company approves the self-assessment report, and it is kept as part of the company's records.

第八條 個人資料保護管理

本公司應依本政策建立「個人資料檔案安全維護及業務終止後個人資料處理辦法」，並授權 總經理核定，修正時亦同。

Article 8 **Personal Information Protection Management**

The company should establish “Guidelines for the Security and Maintenance of Personal Information Files and the Handling of Personal Information after the Termination of Business” based on the Policy and have it approved by the president. The same applies to revisions.

第九條 附則

其餘未盡事宜，悉依主管機關法令及本公司相關規範辦理。

Article 9 **Additional Provisions**

Matters not covered in the Policy should be handled based on regulations set by regulatory agencies and the company's related rules.

第十條 施行及修訂

本政策經本公司董事會核定並依本公司「章則制定政策」公告施行，修正時亦同。

Article 10 Implementation and Revision

The Policy is to be published and implemented in accordance with the Company's policy on establishing rules and guidelines after being approved by the Company's board of directors. The same is true for revisions.

Table: Revision History

Version	Date of Approval	Effective Date	Approval Level	Note:
01	2012/08/24	--	Board of directors	5th board, 7th meeting
02	2014/01/21	--	Board of directors	5th board, 15th meeting
03	2016/08/25	--	Board of directors	6th board, 13th meeting
04	2019/03/21	--	Board of directors	7th board, 10th meeting
05	2019/11/21	2019/11/29	Board of directors	7th board, 14th meeting
06	2020/07/22	2020/07/29	Head of Risk Management Division	This revision did not involve substantive changes, and it was therefore approved by the division-level head of the unit responsible for the Policy in accordance with the Company's policy on establishing rules and guidelines.
07	2023/04/13	2023/04/14	Head of Risk Management Division	Amendment on format and wordings pursuant to "The Policy for the formulation of the Internal Rules and Regulations" of the Company involving no change of substance