富邦金控

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

Document No.	:	FHC-O-PIM-1-20191121
Approval Date	:	2019/11/21
Effective Date	:	2019/11/29
Responsible Unit	:	Risk Management Division, Operational Risk Management Department
Version	:	Version 5

富邦金控

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.

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.

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.

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.

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.

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," the company's "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 Holdings 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 an processing;
12. Should identify internal and external interested parties and their requirements for the protection and governance of personal information of the Company.

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.

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.

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.

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