



AIRA & AIFUL Public Company Limited

90 Cyber World Tower Bldg., 833rd/ 834th Floor, Ratchadapisek Rd., Huai Khwang, Bangkok 10310
Registration Number: 0107557000489
Website: www.aira-aiful.co.th

Personal Data Protection Policy (Revision B.E.2567)

AIRA & AIFUL Public Company Limited



Personal Data Protection Policy (Revision B.E.2567)

AIRA & AIFUL Public Company Limited

A. Reason for the Issuance of the Policy

In order to comply with Personal Data Protection Act B.E. 2562 (PDPA) including amendment, rule, regulation, announcement, guidelines and order of the Office of Personal Data Protection and/or related government offices, AIRA & AIFUL Public Company Limited (hereafter called "the Company") deems it appropriate to set forth the personal data protection policy to be standard in defining guideline, criteria and practice to protect personal data of customers, trade partner, contact partner, shareholder, director, management, staff and/or employee of the company including any person conducting the transaction with company.

B. Objective

1) To comply with the provisions of the Personal Data Protection Act B.E.2562 and additional amendments regarding collection, use, and disclosure of personal data and the provisions regarding data subjects' rights.

2) To protect personal data effectively and adhere to the same standard practices throughout the organization.

C. Scope of Enforcement

This policy shall apply to data obtained from data subjects and other sources as well as third parties who contact and conduct transactions with the Company, regarding collection, use and disclosure of personal data obtained through work activities and prevent personal data from leaking to the public or uninvolved third parties or any personal data breach including to prevent complaints from the data subject.



Section 1

General Articles

Clause 1. Definitions

“Company” means AIRA & AIFUL Public Company Limited.

“Employees” means an employees of AIRA & AIFUL Public Company Limited at all levels.

“Personal Data” means any information relating to a person, which enables the identification of such Person, whether directly or indirectly, such as name, surname, age, date/month/year of birth, national ID numbers, telephone numbers, address, email, photo, etc., but not including the information of the deceased Persons in particular.

“Sensitive Data” means any personal data pertaining to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or of any data which may affect the data subject in the same manner, as prescribed by the Committee, is prohibited, without the explicit consent from the data subject, except where consent a data subject is exempted as required by law.

“Data Protection Officer” means single person or working team which has been designated as Data Protection Officer (DPO) with duties as specified in the Personal Data Protection Act B.E. 2562 (2019) that may have further amendments.

“Processing of Personal data” means Collection, use, disclosure of personal data under the Personal Data Protection Act B.E. 2562 (2019) that may have further amendments.

“Loan” means the granting of a personal loan as part of the Company's business activities.

Clause 2. Legal Department shall be the acting person in charge and in control of compliance with this policy, which includes examination and evaluation of rules, regulations, requirements, manuals and/or any practice guidelines in order to ensure the successful implementation of this policy by submitting requests for approval to authorized persons in line with the Company's delegation of authority policy.

Clause 3. Collection of Personal Data

The company shall collect personal data as follows.

- 1) Data able to identify person such as name, address, birthday, nationality, ID number, contact location, mobile phone numbers, photos, etc.
- 2) Contact information such as address, email, telephone numbers, etc.



- 3) Financial or Transactional Information such as bank account numbers, A money card numbers, revenue information, transactional record, etc.
- 4) Technical information such as IP address, Log, Location data, etc.
- 5) Sensitive Data that the Company shall collect when the Company received an explicit consent from a data subject unless the laws allow to collect without consent.

Section 2

Duty and Responsibility

Clause 4. Duty and Responsibility

4.1 **Board of Directors** is responsible for formulating policy and approving the Personal Data Protection Policy, and provide the company to have an efficient control system, and support the protection and supervision of personal data, including communicating the policy to employees at all levels of the company and outsiders for acknowledgment, in order to achieve practical implementation and to ensure that the company recognizes the importance and all sectors have implemented it until it becomes culture of the company.

4.2 **Data Protection Officer** is responsible for the followings;

1) To provide recommendations to the Company including employees or vendors of the Company regarding overseeing the Company's operation relating to the Personal Data Protection Act B.E.2562 including relevant laws and regulations.

2) To oversee the Company's operation including employees or vendors of the Company regarding collection, use, and disclosure of personal data in accordance with the Personal Data Protection Act B.E. 2562 including relevant laws and regulations.

3) To coordinate and cooperate with the Office of Personal Data Protection Committee in cases where there are problems with the collection, use, or disclosure of the Company's personal information. including employees or contractors of the company in compliance with the Personal Data Protection Act B.E.2562, including related laws and regulations.

4) To maintain the confidentiality of personal data that is known or obtained in the course of performing duties.

4.3 **Directors, Executives, Stakeholders and Employees at all levels** are obliged to strictly follow the policy.



Section 3

Acquisition and Processing of personal data

Clause 5. The Company collects personal data from the following sources;

5.1 Directly from the data subject, the Company may collect personal data from the following cases.

- 1) Loan application, Service Application, Know Your Customer, Signing Contract procedures
- 2) Filling in form, Survey, Registration Form, Complaint filing process or any rights requests
- 3) Contacting via any channels such as telephone, email, social media account, meeting, event,

etc.

- 4) Using Company's websites or A money Mobile Application.

5.2 Personal Data Form other sources as follows;

- 1) Business Partners
- 2) Data from general searching such as public disclosure, internet, government agencies or other organizations etc.

In this case, the Company shall notify a Data Subject without delay, but there should be not exceed 30 days from the date that the Company collects personal data from such source, including conducting to receive data subject's consent for such collection, except where such case is exempted from requesting consent or notifying a data subject as provided by laws.

Clause 6. Processing of Personal data must comply with the Company's objectives that have informed to a Data Subject or to be accordance with laws only, except where processing of personal data for any objectives that is exempted from requesting data subject's consent.

Section 4

Retention Period of Personal Data

Clause 7. The Company will retain personal data for as long as necessary to fulfill the purposes of collection, use, or disclosure of such personal data. The Company may continue to retain personal data for the necessary period to comply with legal requirements or statutes of limitations, or to establish, exercise, or defend legal claims. For example, this period may extend to 10 years from the termination of the relationship. In the case of criminal records, the Company will retain such data for a period of 6 months from the completion of the relevant process.

Upon the expiration of the retention period for the collection, use, or disclosure of personal data, or when it is no longer necessary to retain the data for the purposes of collection, use, or disclosure, the Company will



delete, destroy, or anonymize the personal data in a manner that ensures the data cannot be used to identify the individual to whom it pertains.

Section 5

Data Subject's Rights

Clause 8. A data subject is entitled to request the Company to proceed as the followings;

1) **Right to withdraw consent**, the data subject shall have the right to withdraw the consent to collect, use or disclose personal data that the data subject had already given a consent to the Company at any time.

2) **Right to request access the personal data**, the data subject is entitled to request access to obtain copy of the personal data related to him or her, which is under the responsibility of the Company or to request the disclosure of the acquisition of the personal data obtained without his or her consent.

3) **Right to rectification of personal data**, the data subject shall have the right to request the Company to ensure that the personal data remains accurate, up-to-date, complete, and not misleading.

4) **Right to request to erasure of personal data**, the data subject shall have the right to request the Company to erase or destroy the personal data or anonymize the personal data to become the anonymous data, which cannot identify the data subject for some reason.

5) **Right to request to restrict the use of personal data**, the data subject shall have the right to request the Company to restrict the use of personal data for some reason.

6) **Rights to request to transfer the personal data**, the data subject shall have the right to request the Company to send or transfer the personal data to other data controllers or directly obtain it from him or her for some reason.

7) **Rights to object the collection, use or disclosure of the personal data**, the data subject shall have the right to object the collection, use or disclosure of the personal data for some reason.

Clause 9. A data subject can contact the Company's Data Protection Officer for the above proceeding of data subject rights request, or a data subject can read the details, conditions, and exemptions of any rights on the Company's website.

However, the above proceeding of data subject rights request, the Company shall consider and notify a result of such data subject rights request within 30 days from the date that the Company receives such request.



Section 6

Maintaining Security Measures

Clause 11. The Company will provide appropriate security measures to prevent unauthorized loss, access, use, change, modification, or disclosure of personal data, and will review those measures as necessary or when there are technological changes to ensure effective and appropriate security.

Clause 12. In cases where the Company engages third parties or individuals to collect, use, or disclose personal data on its behalf, the Company will require such third parties or individuals to maintain the confidentiality and security of the personal data. This includes preventing the unauthorized or unlawful collection, use, or disclosure of the personal data for any other purposes.

Section 7

Cross-Border Personal Data Transfer

Clause 13. The Company may transfer or transmit personal data to foreign countries, provided that the destination country or international organization receiving the personal data has adequate data protection standards in accordance with the criteria set forth by the Personal Data Protection Committee's regulations. Unless exempted by law, The Company may also transfer or transmit personal data to recipients located abroad within the same group of enterprises or businesses. In such cases, the Company and the recipients will implement Binding Corporate Rules (BCRs) for data protection within the same group of enterprises or businesses. These BCRs must be reviewed and certified by the Office of the Personal Data Protection Committee before any transfer or transmission of personal data occurs.

Section 8

Penalties

Clause 14. Employees, executives and / or the person who is responsible for the operation of any matter under their duties if ignore or neglect to command or not to perform or order or perform any of their duties causes violation of policies or practices regarding personal data leading to violate the law or any damage. Employees, executives and / or the responsible person, that person must be disciplined according to the company's regulations or must be responsible for the said act according to the offense that occurred. Therefore, in case that such offense causes damage to the company and/or other person, the Company may consider legal proceedings.



Section 9

Other

Clause 15. This policy must be reviewed and updated at least once a year, considering the criteria and methods announced by the Personal Data Protection Committee, including other rules, regulations, and announcements. that may occur in the future that affect personal data protection.

Clause 16. Records of Amendment

Records of Amendment/Adjusted Content

Revision No.	Effective Date	Amended/Adjusted Content	Page
-	21 May 2020	First Announcement	-
1	7 August 2024	Amended and added Reason for the Issuance of the Policy, Objective, Scope of Enforcement	2
		Amended and added Section 1 General Articles Clause 1. Definitions	3
		Added Section 2 Duty and Responsibility	4
		Amended and added Section 3 Acquisition and Processing of personal data	5
		Amended and added Section 4 Retention Period of Personal Data	5
		Amended and added Section 5 Data Subject's Rights	6
		Amended and added Section 6 Maintaining Security Measures	7
		Amended and added Section 7 Cross-Border Personal Data Transfer	7
		Amended and added Section 9 Other	8