

Privacy policy notice for employees and job applicants

AIRA & AIFUL Public Company Limited

AIRA & AIFUL Public Company Limited (“the Company”) is aware of the privacy rights of third parties who contact or have business relationships with the Company. Therefore, this Privacy Policy notice is provided to inform you of the collecting, using and disclosure of personal data of natural persons which is in accordance with the Personal Data Protection Act B.E. 2562 (“Personal Data Protection Act”) and other relevant laws or regulations.

This Privacy Policy notice will inform you of the collection, use or disclosure of your personal data, the type of data, the purposes of processing, data retention period, disclosure of personal data to third parties, your rights, as well as the confidentiality and security of your personal data and contact channels.

1. Who does this announcement apply to? and source of personal data

1.1 This announcement applies to any person that the Company has relationship and is the data subject that the Company has to manage in recruiting and contracting, compensation and performance management, payroll and welfare, benefit management labor relation and communication management, training and development ,encouraging employees to obtain professional license and certificate, succession plan and high potential personnel management, working relationship which means the following persons (“you”)

- (1) Job applicant
- (2) Employee, including short-term employee
- (3) Consultant
- (4) Company director
- (5) Contractor
- (6) Employee of outsource company.
- (7) Internship
- (8) Speaker and Coordinator
- (9) Any person that company obtains personal data (such as family members, referral, guarantor, beneficiary, emergency contact person or other related person)

1.2 Source of personal data

The Company may collect your personal data from various sources as following:

Source of data	Example
1) Receive personal data directly from you	<ul style="list-style-type: none"> • Company internal procedure for your employment contract, when you sign on employment contract, employee insurance procedure and claim. • Contact company through various channels such as telephone, e-mail. • Company's online storage system, such as when you access website or company internal system.
2) Receive your personal data from other sources.	<ul style="list-style-type: none"> • Government agencies such as Royal Thai Police, Anti-Money Laundering office and Court. • Hospital that performs health check-up for new employee. • Your employer company (for employee from outsource company)

2. Personal data that the Company collect, use, or disclose

2.1 What is personal data?

Personal data means any information relating to an individual from which an individual can be identified either directly or indirectly, but does not include the information of the deceased.

2.2 Personal data that the Company collects, uses, discloses or process.

The Company collect various types of personal data including as following.

Type of data	Example
1) Personal data	<ul style="list-style-type: none"> • Title, first name, middle name, last name, nickname, pseudonym, or name that used to take in the past including signature • Photo, face image, or physical appearance.

Type of data	Example
	<ul style="list-style-type: none"> • Gender, height, weight, birthday, age, nationality, marital status, family status, number of family members and number of children. • Information about hobby and interest, photo, language skill. • Information on documents issued by government agencies such as copies of ID card, copy of passport, copy of house registration, copy of driving license, number of professional license, registration number of foreigner.
2) Educational information	<ul style="list-style-type: none"> • Educational qualification and admission, license, membership with professional organization, educational result, training certificate.
3) Contact information	<ul style="list-style-type: none"> • Postal address of home/residence, delivery address, phone number, fax number, personal email. • Postal address of company, company phone number and company fax number, your company email.
4) Employment information	<ul style="list-style-type: none"> • Detail about employment, employment status and employment history such as occupation, position, affiliation, company name or work permit status, name and number and age of previous provident fund member. • Detail about work permit, check information about reference person and background, tax identification number. • Employment history (including detail about salary, work attendance and various benefits), date of employment start, service years of employment, termination of employment, possession assets during employment, various assessment (performance and possibility assessment, assessment about different types of competency, operational knowledge and leadership (behavioral) skill, including technological assessment and use of various technology (such as Internet, e-mail),

Type of data	Example
	including information about disciplinary action and indemnify.
5) Financial information	<ul style="list-style-type: none"> • Bank account number. • Credit history and detail about using Bank. • Claim history under insurance contract. • Income / Salary / Service fee / Other compensation. • Employee salary deduction according to legal requirement. • Voluntary payroll deduction. • Financial assistance (such as benefit, welfare, assistance, grant, subsidy).
6) Technical information, equipment or tools	<ul style="list-style-type: none"> • Computer serial number (IP address or Mac address) • Cookies (Cookies ID) • Model and type of device, network, connection information. • Log and Log-in information, access timing. Use and duration of use of application and website, search history, browsing data • Browser plug-in type and version. Operating system and platform including other technologies on device which you use to access platform. • Other technical information from use on platform and operating system.
7) Sensitive Personal Data	<ul style="list-style-type: none"> • Company may collect your sensitive personal data such as criminal history, health information and biometric information therefore company must get your consent clearly or as required by law.
8) Other information	<ul style="list-style-type: none"> • Such as giving opinion, feedback, complaint, advice, survey response, inquiry and information that you voluntarily provide during communication with human resource department.

If you don't provide your personal data to company, the Company may not be able to offer you a position on request and Company may not be able to

perform all duties under employment contract/compensation management/benefit management/payroll, wage and benefit/Training and Development/ Scholarship /Supporting employees to obtain professional license and certificate/ Management of succession plan and high potential personnel, working relationship or unable to perform company obligation under the law.

3. Personal data for third party

If you provide personal data of other persons to Company such as Information about reference person, spouse, family members, children, patron, dependent, member of Board of Director, director, shareholder, representative, chief of manager, guarantor, beneficiary, or you may request Company to disclose personal data of such persons to third parties.

You are responsible for notifying detail of this announcement to such person as well as getting consent from such person (if consent is required). In addition, you also have duty to proceed for company to collect, use or disclose personal data of those persons in accordance with law as stated in this announcement.

4. Objective on collection, use or disclosure of personal data

Company will collect your personal data as necessary according to objective as following.

Objective for collecting, using or disclosing personal data	Lawful basis
1) To proceed recruitment process such as recruiting, selection, hiring decision, processing of job application, job interview, evaluation of qualification based on information contained in job application, suitability and qualification as well as work performance, checking background and screening in case you get offer a job, checking your information with list of prohibited persons, approval of job application, contacting you about position that you are requesting or applying for (contacting you to notify that your application has been approved or rejected).	<ul style="list-style-type: none"> • Consent • Consent for sensitive personal data.
2) To proceed related to employment contract between company and you including other	<ul style="list-style-type: none"> • The performance of a contract or proceed

Objective for collecting, using or disclosing personal data	Lawful basis
contracts related to employment such as non-disclosure agreement.	as request before entering into a contract.
3) To perform company's duty under employment contract and other steps related to employment such as salary preparation, employee history record, disabled person employment, all types of leave report preparation, working performance evaluation, assessment and confirmation of work in probation period, applying for provident fund and information management about fund.	<ul style="list-style-type: none"> • The performance of a contract. • Comply with law. • Consent for sensitive personal data.
4) To comply with legal obligation and law enforcement request including report information to government agencies as required by law, such as Revenue Department, Social Security Office, Department of Labor Protection and Welfare or when receiving a summon or a writ of attachment from police, government agencies or court.	<ul style="list-style-type: none"> • Comply with law.
5) To encourage you to comply with requirement under employment contract as employee of company including using blood vessel scan data to maintain security of company systems and data for complying with your employment contract.	<ul style="list-style-type: none"> • The performance of a contract. • Consent for sensitive personal data.
6) To manage any matters related to health and insurance such as conducting health check, health insurance, other types of insurance and insurance claim.	<ul style="list-style-type: none"> • The performance of a contract. • Consent for sensitive personal data.
7) To conduct training for employees as agreed or stipulated in employment contract and company policy, rules and work regulation and relevant law.	<ul style="list-style-type: none"> • The performance of a contract. • Comply with law.
8) To maintain security inside or around head office, branch office or company premise through the closed-circuit television system (CCTV).	<ul style="list-style-type: none"> • Legitimate interest
9) To support loan and/or applying for your credit card by providing employment status information to commercial banks.	<ul style="list-style-type: none"> • Consent

Objective for collecting, using or disclosing personal data	Lawful basis
10) To handle and resolve complaint from working performance under employment contract including investigation or other legal process.	<ul style="list-style-type: none"> • The performance of a contract. • Comply with law.
11) To establish legal claim according to law, compliance or the exercise of legal claim or raise as defense against legal claim.	<ul style="list-style-type: none"> • The performance of a contract. • Legitimate interest • Legal claim for sensitive personal data.
12) To retain your information after termination of employee status and to refer for your job re-application with company in the future.	<ul style="list-style-type: none"> • Consent
13) To disclose your information to customers, partners and other third parties due to right and duty to comply with employment contract.	<ul style="list-style-type: none"> • The performance of a contract. • Legitimate interest
14) To disclose your information to agents, service providers or outsources which proceed for company operation.	<ul style="list-style-type: none"> • The performance of a contract. • Legitimate interest. • Consent for sensitive personal data.

5. Retention period of personal data

The Company will retain your personal data if it is necessary for objective of collecting, using, disclosing, or processing personal data which specified in this policy. Criteria to determine retention period are as following:

The Company retain personal data throughout period which company conduct relationship about recruitment, employment contract as well as human resource management with you and Company may continue to retain personal data for necessary period to comply with law or in accordance with legal period or to establish legal claim for compliance or exercise of legal claim or to raise own defense for the exercise of legal claim or for other reasons according to policy and company's internal requirement.

6. Disclosure of data

To proceed according to objective that specified in this announcement. Company may disclose your information to third parties as following.

- (1) AIFUL Corporation in Japan and AIRA Capital Public Company Limited for internal management such as employee's claim management, corruption case investigation inside company.
- (2) Customer, service provider and other third parties due to right and duty to comply with employment contract.
- (3) Agent, Contractor/Subcontractor and/or service provider for any job such as document storage and disposal service provider, printing company, information technology development company, auditor, lawyer, legal advisor, any consultant.
- (4) Government agency, regulator, or other agencies as required by law including official staffs who exercise their legal authority such as the court, police, Social Security Office, Revenue Department, Immigration Office, Ministry of Commerce, Student loan fund.
- (5) External training institution.
- (6) Bank or credit card company which having legal relationship with you.
- (7) Hospital for your health check-up.
- (8) Insurance company.
- (9) Provident fund management company.

7. International transfers of your personal data (if any)

The Company may need to transfer your personal data to third parties located in foreign country such as Japan for company to achieve business objective or for your benefit and company benefit such as when corruption occurs within organization or have complaint from employees.

When it is necessary for the Company to transfer your personal data to third country which has standards for personal data protection not comparable to Thailand. The Company will take steps to provide adequate personal data protection measures for personal data transferred, or in order for the transfer to be carried out in accordance with applicable personal data protection laws, for example, the Company may request that third parties granted access to the personal data that have been transferred, agree with the Company to certify that the data will be protected in accordance with personal data protection standards that are equivalent to those in Thailand.

8. Use of cookies

The Company may collect and use cookies and similar technologies when you use our products and/or services including the use of the website and A Money application.

The collection of cookies and similar technologies will allow the Company to recognize you, know your preferences and improve the way the Company offers products and/or services to you. Please see details in Notice on the use and management of cookies (Cookies Notice) https://www.amoney.co.th/privacy/cookie_consent and http://www.aira-aiful.co.th/?page_id=1739

9. Collection and use of personal data for the original purpose

The company has the right to collect and use your personal data as the company has collected before the date the Personal Data Protection Act B.E. 2562 continues to come into force for the original purpose. You may at any time withdraw your consent to the collection and use of your personal data for the original purpose. (please see details in the section on **Rights of personal data subject**)

10. Rights of personal data subject

10.1 You have rights under the Personal Data Protection Act to do the following:

- (1) Right to withdraw consent : You have the right to withdraw your consent to the collection, use or disclosure of personal data that you have given us your consent to at any time during the period that such personal data is with the Company.
- (2) Right to access to personal data : You have the right to access your personal data and request the Company to make a copy of such personal data for yourself, including request the Company to disclose the acquisition of personal data that you did not give consent to the Company.
- (3) Right to rectification of personal data : You have the right to request the Company to correct personal data to be accurate, update, complete and not misleading.
- (4) Right to erasure : You have the right to request the company to delete or destroy or make the personal information non-personally identifiable for some reason.

- (5) Right to restriction : You have the right to suspend the use of your personal data for some reason.
- (6) Right to transfer : You have the right to request the transfer of your personal data that you have provided to the Company to another data controller or yourself for some reason.
- (7) Right to object : You have the right to object to the collection, use or disclosure of your personal data for some reason.

10.2 Channel for exercising rights

You can exercise the above rights as data subject at the head office or send a letter via the postal address of the Company with the following documents.

- 1) Exercise rights request form with a signature (You can download such documents through the Company's website)
- 2) Copy of ID card with signature certifying true copy.

However, if the Company refuses to exercise your rights, the Company will inform you of the reason for the refusal.

10.3 Processing period

The company will process your request to exercise your rights within 30 days after receiving the complete exercise request form with complete supporting documents. During the aforementioned operation, your personal data stored in the Company's database will not be changed in any way and may still be collected, used and/or disclosed.

11. Measures for the security of personal data

11.1 The Company will provide appropriate security measures in order to prevent unauthorized or improperly access, use, change, correct, loss, destruction or disclosure of personal data.

11.2 If the company discloses personal data to a data processor, the Company will supervise other persons entrusted by the Company to process personal data as instructed or on behalf of the Company appropriately and in accordance with the law.

12. Contact information

In case of doubt or wanting more information about the protection of your personal data, Collection, use or disclosure of your data, exercise of your rights or have any complaints, you can contact the company as follows:

AIRA & AIFUL Public Company Limited and Data protection offer (Mr. Yuji Fukada)

Address: 90 CW Tower, Floor 33,34, Room No. B 3301-2, B 3401-2, Ratchadaphisek Road, Huai Khwang Sub-district, Huai Khwang District, Bangkok 10310

Tel : 0-2117-5000

E-mail: DPOoffice@aira-aiful.co.th

In this regard, you have the right to complain to the relevant Personal Data Protection Committee when the Company violates or fails to comply with the Personal Data Protection Act including rules or other announcements issued under the said Act.

13. Amendments to the Privacy Notice

The Company may from time to time review and may amend this notice as appropriate to ensure that your personal data is properly protected. If this notice is amended, the Company will notify you through the website or by other appropriate methods.

Announce as on 27 April 2022