

	Golden Lime Public Company Limited		
	Personal Data Protection Notice for Employees and Job Applicants	Document no.	Revision no.
		CS20181101/WI01_EN	Rev.1
		Date Version	Total Pages
		10/11/2022	7
			Download PDPA policy CS20181101_EN
			

Personal Data Protection Notice for Employees and Job Applicants
Golden Lime Public Company Limited and Subsidiaries Company

Parties	Employees and Job Applicants
Scope of Application	A person who engaged or to be engaged in an employment contract (either part-time or full time including current employees) or interns (hereinafter wholly referred to as “employees”). Plus, persons apply for a job of the Company. (“Job Applicants”)

Golden Lime Public Company Limited and affiliates do respect the privacy of employees. To ensure your personal data is protected, therefore, a personal data protection practice guideline has been established to provide details regarding the collection, use, retention and disclosure (all referred as “processing”), as well as the deletion and destruction of your personal data as required by the Personal Data Protection Law.

This Code of Practice includes: the details of the collection, use and/or disclosure of your personal data as an employee, job applicant of the Company and set out the basic principles of personal data protection. The practice guidelines cover operations of Golden Lime Public Company Limited in relation to your personal data and other relevant information as below listing;

1. Purpose of collecting, using, disclosing and/or transferring personal data abroad

The Company will collect, use and/or disclose information in general including your personal data only for legitimate interests of the Company with your consent or for other legitimate reasons, as necessary for the following purposes

- recruiting and selecting job applicants
- approving salaries and benefits for the Company's employees
- employment-related purposes and the contracting employees to work such as a physical examination before entering the workplace, identifying the beneficiary's name, registration of the insurer, criminal background check, entering into an employment contract, establishment of employee records, employee registration and other relevant human resource functions, etc.
- welfare and employee benefits management including insurance claims, sending the list of employees to hospitals for annual health check-ups or for the hospital to forward health check-up data to the company
- recording working hours, salary , wages, bonuses, compensation payment or any other benefits.
- complying human resources laws and lawful orders of government agencies
- evaluating employee performance
- training management.
- job rotation, moving an employee to a new relevant role
- forwarding information to affiliates for accounting audit and internal control system audit
- human resource management such as disciplinary action, termination of employment, resignation and retirement, etc.
- communicating with applicants and relevancies to applicants.



- establishing lawsuits, compliance or exercise of legal claims ,class actions, counterclaims which are subject to various legal steps
- monitoring the public order and security of persons and company assets
- disclosure on personnel performance, results of personnel development and training or information related to the activities of HR operations or social activities Including the company's sustainability driving development initiatives disclosed in an annual report and/or on the Company's website and/or various media or communication channels or social media channels or application communication of the group of companies or the main shareholder group of the company

However, if you refuse to provide personal information that is required for compliance with laws or contracts or to enter into contracts with the company may impair the performance of the contract and the right to access welfare or services provided by the Company. This may cause incomplete process failing facilitation and communication which may affect your work.

2. Sources of Personal Data

- **General Personal Data**, such as first name, last name, job position, date of birth, address, telephone/fax number, email address, photographs, motion images from video recording or closed-circuit television (CCTV), audio recordings from meetings, information on the national identification card or passport, household registration documents, signature, social media account information (such as the LINE ID), car information (such as the car plate number, brand, model, and color), and other Personal Data you provide to the Company.
- **Sensitive Personal Data** is health data for the purpose of disease screening (including the COVID-19) upon your visit or entry into the Company's premises or operating areas, disability details, which the Company needs to obtain consent from a data subject or as much as necessary and permitted by laws.
- **Technical data**, such as the username and password to access the system, IP address, Media Access Control data, log files, cookies data, system usage data, website usage data, operating systems and platforms, and other technologies on devices used to access the platform, as well as other Personal Data regarding the use of the Company's system.

Others' personal data includes the first-last name and telephone number of the father, mother or guardian, contact person, guarantor, and other personal information you provide to the Company.

If you have provided personal data of another person to the Company as stated above ,you should ensure that you have the authority to provide such personal data and has the power to allow the Company to process such personal data in accordance with this notice. You also have a duty to notify those persons of this notice and/or to obtain their consent if required by law or referred to other legal bases.

Personal Data collection

1) related information and documents to the recruiting process such as resume ,curriculum vitae (CV), cover letter, job application, recruitment process feedback.

2) employee contact information such as name, surname, address, telephone number, email, social media information.



3) information about the employee's identity such as date of birth, age, gender, marital status, interests, opinions.

4) information about family members or dependents of employees who are eligible for welfare under the Company's regulations and personnel management regulations such as information about their spouses, the child Information about parents beneficiary. Employees shall also notify this policy to dependents,

5) photos and motion image

6) information on education, competence, and potential development and other qualifications of employees such as educational level, educational background, institution/university educational record, training history, educational performance results, test results, legal rights to work, professional qualifications, language proficiency and other capabilities, references that employees have provided to the company.

7) past work experience such as job titles, employer details, salary and compensation welfare

8) work location

9) military status

10) employee characteristics such as habits, behaviors, attitudes, aptitudes, skills, leadership the ability to work with others, emotional intelligence, corporate commitment which may be obtained through observations and analyzes made by the Company and our employees during our operations or participation in activities.

11) information required for reporting to a regulatory agents such as the Ministry of Labor, Stock Exchange of Thailand ,Office of the Securities and Exchange Commission (SEC), Thai Institute of Directors Association (IOD)

12) financial information such as wages, salaries, income, taxes, provident funds, bank accounts, tax exemptions or deductions.

13) information related to social security ,labor protection benefits, welfare and benefits that employees receive or are entitled to receive in accordance with the Company's regulations and personnel management regulations.

14) record of attendance and duration of work overtime, absence and leave

15) work history, job title, meeting attendance, comment input adding the director's biography and registration in case of directorship.

16) usage and access to information systems, computers, operating systems, websites, applications, network systems, electronic devices, e-mail systems, in order to comply with our information technology policy and relevant laws.

17) information collected through participation such as participation in events, survey, assessment



18) information that employees choose to share and disclose through our systems, computers, tools, questionnaires, assessments and company documentation.

19) copies of documents that can be used to identify employees such as ID cards, passports, other documents issued by government agencies, civil registration, diploma, work certificate

20) details of contact person in case of emergency

21) vehicle license ,driving license and in case the driver uses the company's car , his driving behavior will be collected.

22) Other information necessary to investigate conflicts of interest, such as shareholding and relationship with business partners.

23) Information about an accident Both in the event that the employee has an accident during work or due to the operation and other accidents arranged by the Company.

24) Other necessary information for employment contract, welfare and benefits, our analysis and administration, after retirement process and compliance with various laws

25) complaints, grievances, investigations, disciplinary action.

26) **Special types of personal data or sensitive personal data** We may need to collect and process special types of personal data of employees for the purposes stated and may process special types of personal data of employees for following cases

- **Health information** such as weight, height, congenital diseases, physical examination results, medical certificate, medical history for labors' protection and the provision of welfare related to medical treatment for employees, employee competency assessment, complying with relevant laws to analyze employee health data for other appropriate management purposes

- **Biometric data** such as fingerprint data, face image data to be used to identify and verify the identity of the employee, crime prevention and maintaining our legitimate interests or another person

- **Criminal records** collected from the employee or the employee consents to request from the legal authority to consider the suitability of work and to maintain the legitimate interests of the Company or of another person

- **Religious beliefs;** ideology, philosophy, race, nationality, disability, genetic information, biological information in order to provide suitable facilities, activities and welfare for employees to manage employees' care equally and fairly according to human rights principles.

- **Other special types of personal data for lawful purposes**, such as to prevent or suppress harm to a person's life, body or health.

Legal basis for the collection, use, and disclosure of Personal Data

The Company generally collects, uses, discloses, and processes your Personal Data on any of the following legal basis:



- 1) for the performance of a contract, or in order to take steps, at your request, prior to entering into an agreement with the Company;
- 2) for legitimate interests of the Company or a third party to the extent that these interests do not override the fundamental rights in your Personal Data;
- 3) for compliance with a law;
- 4) to prevent or suppress a danger to the life, body or health of a person.
- 5) Other cases permissible by laws.

For collection, use, and disclosure of your Sensitive Personal Data, the Company relies on the following legal basis:

- 1) Upon explicit consent obtained by the Company from the consent form requesting for your consent to the collection, use, disclosure, and processing of your Personal Data;
- 2) Where it is necessary for the establishment of a legal claim, compliance with, or exercise of a legal claim, or to defend a legal claim
- 3) Where it is for vital interests to prevent or suppress any harm to the life, body, or health of a person
- 4) To comply with the law to achieve objectives related to preventive medicine or occupational medicine, medical diagnosis, providing health or social services ,medical treatment, health management, public health benefit, road accident victims protection etc., where the collection of personal information is necessary to perform the duties of the Company or yours.
- 5) information made public with your express consent; or
- 6) Other cases permissible by laws.

We will only process employee's special personal data with the employee's consent or for other purposes as required by law. Sufficient protection measures of special types of personal data of employees are implemented.

3. Retention period

- 3.1 Personal data of employees will be stored only as to achieve the purposes for each type of data unless the law allows for a longer retention period. In the event that the retention period cannot be clearly specified, the retention will be in accordance with the retention standard (e.g., a general legal age of up to 10 years) In the case of applicants who do not pass the selection process, their data will be kept as reference and considered to be retrieved for selection, but not exceeding 2 years
- 3.2 Employees personal data are kept throughout employment as per the contract and for the particular period after the termination of employment
- 3.3 Personal data of family members or custodians of employees are retained for particular period following the purposes stated in the policy. In particular, in response to the employee's right to receive benefits in accordance with the Company's regulations and personnel management regulations.
- 3.4 The Company will only process personal data upon consent in the event that the employee requests to withdraw such consent and the Company shall follow the employee's request.



However, the Company will continue to keep as a record where necessary of that consent withdrawn to respond to further requests in the future.

- 3.5 The monitoring and audit system is in place to carry out the deletion or destruction of personal data when the retention period has expired or is unrelated to or beyond the necessity for the purpose for which the personal data was collected.

4. Personal data enclosure and/or transfer aboard

4.1 The Company is obliged to disclose necessary personal data to affiliates, various service providers and business partners such as insurance companies, insurance agents, hospitals, consultants, hotels, airlines, institutions or training providers, or postal service providers, etc., and for the purposes in clause 2

4.2. Personal data transfer to foreign countries, in some cases, is to be stored and processed by companies located abroad having standardized personal data protection in accordance with the Thailand data protection laws. Data transferred is strictly maintained and secured.

4.3 Types of persons or entities to which the Company discloses your personal data

The Company may disclose your personal data (only as necessary) to third parties or entities for the purposes stated in this notification. Such third parties may be located in Thailand or abroad as following list:

- 1) Affiliates, a joint venture or a group of major shareholders of the company

The Company may share personal data with affiliates of major shareholders or joint ventures for business integration or cooperation. Risk Management exchange information with each other and internal audits of the Group

- 2) Third parties who provide services related to the Company's operations

The Company may disclose your personal data to those who is acting as an auditor, internal control system auditor, financial institution providing credit or financial transaction services, personal data controller or personal data processor. For example, accounting service providers, banks, information technology service providers, Cloud service providers (Cloud), storage or document service providers, application provider, building and parking lots administrator both in the present and in the future, etc.

- 3) Relevant government agencies

The Company may disclose your personal data to government officials and government agencies who legally are authorized to protect the rights of the Company or of others or for your benefit, such as the Department of Investment Promotion, the Revenue Department, the Court of Justice, the Legal Execution Department, etc.

- 4) Other external persons or entities

The Company may disclose your personal data to third parties or entities to access your personal data, for example, professional advisors (such as legal advisors, financial advisor



external auditors) and external agencies that the Company wishes to publicize for the purposes stated above.

5. Improvement to Personal Data Protection Practices

The Company reserves the right to amend this Code of Conduct, whereby the Company will notify you of such amendments. In addition, the Company may notify you of additional details regarding your privacy such as the purpose of collecting your personal data beyond these guidelines.

Any amendments to this Code of Conduct or other details relating to privacy will become effective as soon as the Company has notified you as the Company deems appropriate, except in the case where the Company need to obtain your consent in which such amendments will come into effect just when the Company already obtains your consent.

6. Human Resources Department contact

If you wish to exercise your rights in relation to your personal data or if you have any questions about your personal data under these guidelines, please contact our Human Resources department representative. Submit your request Email: lqpersonal@goldenlime.co.th Tel : 036-436439

As on 10th November 2022

(Mr. Geza Email Perlaki)

Managing Directors

Document revisions

Item	Document number	Revision	Issue date	Remark
1	CS20181101_PM01	Rev.0	Only Thai version	Do not have English version
2	CS20181101/WI01_EN	Rev.1	10 November 2022	To notify, to publicize to all stakeholders
				
	Download this document CS20181101/WI01_EN			