

Announcement
DPO 004/2023
Data Privacy Policy

1. Rationale

Advancements in information and communication technologies allow easy access, collection, usage and disclosure of personal data. This may cause damage to an owner of personal data. Besides, the Personal Data Protection Act B.E. 2562 (2019) (PDPA) was published in the Royal Gazette on May 27, B.E. 2562 (2019).

The Company has realized that data privacy is important and privacy right is one of the fundamental rights which shall be protected under the Constitution of the Kingdom of Thailand and the Universal Declaration of Human Rights. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks. Businesses should support and respect the protection of internationally proclaimed human rights according to the UN Global Compact and the Personal Data Protection Act B.E. 2562 (2019) (PDPA). The Company hereby declares the Data Privacy Policy as follows:

2. Objectives

Data Privacy Policy has been developed for the following objectives.

2.1 To protect the personal data of anyone who transacts, uses services, owns stock in the company, or is affiliated with it. This includes, but is not limited to the list below:

- a. Customers
- b. Employees and applicants
- c. Shareholders, Investors
- d. Creditors, debtors
- e. Suppliers and business partners
- f. Individuals employed by the Company to do specific duties, such as expert consultants and ICT service providers, to mention a few.
- g. Visitors to the Company's website and mobile application
- h. Persons contacting or using the Company's facility or space
- i. Families of employees, beneficiaries following life insurance provided by the Company
- j. Person in reference, such as those mentioned in employment applications, who sell products and services to the Company

2.2 To define roles and responsibilities of business units, executives, employees relating to personal data protection

2.3 To set up procedures or measures for ensuring the security of personal data protection

2.4 To create guidelines for employees involved with personal data

2.5 To build trust in in security of personal data to any personal data owners

3. Scope

3.1 Data Privacy Announcement L&C 28/2019 is no longer in effect. This announcement is now effective.

3.2 This announcement applies to all committees, directors, executives and employees of CP ALL Public Company Limited and its subsidiaries (except CP Aextra Public Company Limited and its subsidiaries) as well as business partners, suppliers, service providers and stakeholders.

4. Definition

“Company”	means CP ALL Public Company Limited and its subsidiaries
“Subsidiary”	means any limited companies or public limited companies under the Company according to definitions in the announcement of the Securities and Exchange Commission
“Personal Data”	means any information relating to a Person, which enables the identification of such Person, whether directly or indirectly, but not including the information of the deceased Persons
“Sensitive Data”	means Personal Data which are sensitive and likely to lead to discrimination including racial origin, religious beliefs, sexual orientation, criminal record, health information, disability, biometric data or any data in accordance with the law
“Data Subject”	means a Person who is the owner of the Personal Data, for example customers, business partners and employees
“Data Controller”	means a natural or juristic person authorized to make decisions on the collection, usage, or disclosure of the Personal Data. This person is the Company or business unit or employee who is responsible for the Personal Data
“Data Processor”	means a natural or juristic person who collects, uses, or discloses the Personal Data by order of or on behalf of the Data Controller. This person

is business partner, third-party person or company hired by the Company.

“Person” means a natural person

“Incompetent person” means minor, incompetent person or quasi-incompetent person under the Civil and Commercial Code

“Data Protection Officer” means a person who is appointed by the Company as the Data Protection Officer (DPO) in accordance with the Personal Data Protection Act B.E. 2562 (2019)

“Data Protection Coordinator” means a person who is appointed as the Data Protection Coordinator (DPC) in accordance with this policy

“Personal Data Protection Law” means laws related to the protection of Personal data in the country where the company operates, such as the Personal Data Protection Act of 2019, to name a few.

5. Personal Data Protection

5.1 Collection of Personal Data

Collection of Personal Data shall be conducted in accordance with the purpose and shall be limited to the extent necessary in relation to the purpose or direct benefits based on the purpose of the collection.

5.1.1 The Data Subject shall be informed the following details prior to or at the time of such collection;

- 1) Purpose of the collection
- 2) Retention period
- 3) Categories of persons or entities to whom the collected Personal Data may be disclosed
- 4) Information or contact details of the Company and Data Protection Officer
- 5) Rights of Data Subject
- 6) Impacts in case that the Personal Data are not provided for compliance with a law or a contract

5.1.2 The personal data shall not be collected without the consent of the Data Subject, unless;

- a) it is for the purpose relating to public interest, research, statistics, or in compliance with the law;
- b) it is for preventing or suppressing a danger to a Person’s life, body or health;
- c) it is necessary for the performance of a contract, or in order to take steps at the request of the Data Subject prior to entering into a contract;

- d) it is necessary for the performance of a task carried out in the public interest, or for the exercising of official authority;
- e) or for legitimate interests of the Data Controller or any other Persons or juristic persons other than the Data Controller, except where such interests are overridden by the fundamental rights of the Data Subject;
- f) it is the legal practice of the data controller;

5.2 Collection of Personal Data of Incompetent Person

In case of collection of Personal Data of a minor for any purposes he is unable to act alone in accordance with the Civil and Commercial Code, such act also requires consent of a person exercising parental power or his legal representative. In case that the minor is below the age of ten years, the consent must be obtained from a person exercising parental power or his legal representative.

In case of collection of Personal Data of an incompetent person or a quasi-incompetent person, the consent must be obtained from his guardian, curator or legal representative.

5.3 Collective of Sensitive Data

The Company shall not collect Sensitive Data, unless it is necessary and the Data Subject has given the consent explicitly, except the case that it is permitted to do so without the consent by the law.

5.4 Usage or Disclosure of Personal Data

Usage and/or disclosure of personal data shall be conducted according to the purpose notified to the Data Subject prior to or at the time of such collection, or shall be limited to the extent necessary in relation to direct benefits based on the purpose of the collection. It shall be conducted with the consent of the Data Subject, except the case that it is permitted to do so without the consent by the law, or in compliance with the law.

Any other Persons or juristic persons who obtain the Personal Data with the consent of the Data Subject, or the Data Processor shall use the Personal Data according to the purpose which the Data Subject has given the consent to the Company and the Person or juristic person has informed to the Company.

6. Quality of Personal Data

Collected Personal Data must remain accurate, up-to-date, complete, and not misleading. The Data Subject shall be provided the access to make request or edit his own Personal Data.

7. The duration of personal data retention and deletion

The Company must establish the retention period for personal data as necessary according to the intended purposes expires, the data must be deleted, destroyed, or anonymized.

8. Role and Responsibility

The Company strictly requires any employees or business units in relation to the Personal Data to realize the importance and take serious responsibility for the collection, usage or disclosure of Personal Data in accordance with the Company's Data Privacy Policy and guidelines. The Company designates the following persons or business units to oversee and monitor any business activities to ensure the compliance of the Company's Data Privacy Policy and the Personal Data Protection Act

8.1 Data Controller

8.1.1 To establish appropriate security measures of personal data protection and regularly review them to ensure the effectiveness and keep up to date with latest technologies

8.1.2 To determine scope of processing Personal Data disclosed to any other Persons or juristic persons

8.1.3 To set up monitoring system for Personal Data processing in compliance with the law

8.1.4 To keep records relating to Personal Data in accordance with the law

8.1.5 To make agreement with Data Processor, any juristic persons or third-party persons that in case of Personal Data disclosure to hired Data Processor, juristic persons or third-party persons, all of them must ensure security measures are in place for the collection, usage and/or disclosure of Personal Data is processed in accordance with this policy and the Personal Data Protection Act.

8.2 Data Processor

8.2.1 To process collection, usage and/or disclosure of personal data by order of the Data Controller

8.2.2 To set up appropriate security measures for personal data

8.2.3 To process and keep records of personal data processing activities

8.3 Data Protection Officer

8.3.1 Develop and review personal data protection policy, inclusive to the Company's personal data protection guideline, ensuring completeness and legal compliance.

8.3.2 To give advices on personal data protection to the Company's executives, employees and business partners

8.3.3 To monitor performance of the Data Controller and the Data Processor

8.3.4 Govern different functions within the Company, subsidiaries and supplier companies to ensure compliance according to the Company's personal data protection policy and guideline

8.3.5 Report performance of different functions within the Company, subsidiaries and suppliers to Management officers

8.3.6 Facilitate grievance or usage requests of personal data owners as contacted by personal data owners

8.3.7 To coordinate and cooperate with Office of the Personal Data Protection Commission in case of issues on collection, usage or disclosure of Personal Data of the Company, subsidiaries and business partners

8.3.8 Notify Office of the Personal Data Protection Commission regarding the violation incidents of personal data protection within 72 hours after the incident came to attention

8.4 Corporate Legal Office

8.4.1 Provide consultation, suggestion and feedback regarding operating in full compliance to personal data protection laws

8.4.2 Monitor/produce relevant contracts to ensure compliance to personal data protection laws

8.5 Risk Management Function

8.5.1 Search and identify risks within different function's activities or operations among relevant companies relating to collection, usage and/or disclosure of personal data

8.5.2 Conduct risk assessment by stipulating the risk level of each activity or operation, as well as identifying risk appetite

8.5.3 Follow up to ensure each function is operating within risk appetite

8.5.4 Review risk level of each function's activities and operation quarterly

8.5.5 Develop reports and report risks to Executive Officers

8.6 Internal Audit Office / External Audits

8.6.1 To audit performance of persons involved with Personal Data processing

8.6.2 Internal audits review documents, process and conduct efficiency assessment on security level relating to personal data

8.6.3 Organize for reviews of documents, processes and efficiency assessment on security level relating to personal data. External auditors shall conduct it annually.

8.6.4 To report the audit result to the Company's Audit Committee

8.7 Subsidiaries, Office Level or Equivalent

8.7.1 The highest-level executives of subsidiaries or offices or equivalent shall be responsible for commanding, controlling and overseeing to ensure that all employees strictly comply with the Personal Data

Protection Act B.E. 2562 (2019) and this policy. They are appointed as Data Protection Coordinator (DPC) who shall report any personal data breaches occurred in their organizations or offices to the Data Protection Officer (DPO).

8.7.2 Subsidiaries, command lines, office level or equivalent shall be able to establish rules and regulations on data privacy within the organization. Any rules and regulations shall be in compliance with this policy and the Personal Data Protection Act and also notified to Legal Office, Business Function.

9. Security

The Company stipulates that its employees and external contractors must strictly adhere to ensure the personal data privacy and security, the Company establishes the measures as follows;

9.1 Determine the right to access, use, disclose, or process Personal Data as well as identity verification procedures of any individuals who access or use the personal data. Establish security measures including review and assessment procedures in compliance with the Company's Information Technology Security Policy.

9.2 To send or transfer the Personal Data to a foreign country, or collect the Personal Data in any databases of the service provider located in a foreign country. The destination country that collects such Personal Data shall have the personal data protection measures as good as or better than ones in this policy.

9.3 In case of violation of the Company's security measures which may cause a Personal Data breach. The Company shall proceed according to Data Breach Handling Policy and legal requirements. If such Personal Data breach is likely to result in a risk to the rights and freedoms of the Data Subject, the Company shall also notify the Personal Data breach and the remedial measures to the Data Subject without delay. The Company shall not take any responsibilities in case that the Data Subject or any other persons who obtain the consent from the Data Subject fails to comply with the security measures due to his own intention, negligence, or ignorance and causes the Personal Data to be used by or disclosed to a third party or any other persons.

10. Rights of Data Subject

The Data Subject shall have the rights regarding his Personal Data including to request access to, to obtain copy, to withdraw consent, to object to the collection, usage or disclosure, to erase or destroy or stop using, to update, to complain, to request to transfer to other Data Controllers, unless it is likely to impact other Persons' rights and freedoms, to perform for reasons of public interests or for compliance with the law, or to conduct research. Any actions shall be performed in compliance with the Personal Data Protection Act.

11. Complaint and Misconduct Report

If it is suspected or believed that a personal data breach has occurred regarding collection, usage and/or disclosure of personal data or personal data owners needing to file grievances or utilize personal data owners'

rights. This would be in accordance to the policy, or Personal Data Protection Act. Personal data officers can be contacted at the following details.

Personal Data Officer

CP ALL Public Company Limited

Address: 313 C.P. Tower 24th Floor, Silom Road, Silom, Bangrak, Bangkok 10500

Email Address: privacy@cpall.co.th

Telephone: 02-826-7744

12. Training

The Company shall provide training and evaluation on compliance with the Personal Data Protection Act to all executives and employees. The Data Protection Coordinator (DPC) must attend the training and ensure that all employees in relation to the Personal Data shall attend the training.

13. Policy Review


The Company shall review the Policy on at least an annual basis or in case of any changes in the law.

14. Punishment

The Company shall not compromise in personal data protection. In case the data controller, data processor or any responsible relating to personal data protection neglects to conduct, command or follow their duties, resulting in collection, usage and/or disclosure of personal data in violation of personal data owner. This is a violation of the Data Privacy Policy and guidelines and/or the Personal Data Protection Act, which stipulated the following. The personnel must be penalized according to the Company's regulations. If the offense of the personnel or other persons causes damages to the Company and/or any other persons, the Company may consider additional prosecution action.

This new policy will be effective from 1 September 2023 onwards.

Announced on 1 September 2023.



(Mr. Korsak Chairasmisak)

Chairman of Executive Committee