CP ALL Public Company Limited

Data Privacy Policy Announcement

Doc. No. L&C 28/2562

---

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

The Data Privacy Policy has been established to protect personal data which an owner provides for transaction processing, services, stakeholder or involvement in the Company with the following objectives;

2.1 To define roles and responsibilities of business units, executives, employees relating to the personal data

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

2.3 To create guidelines for employees involved with the personal data

2.4 To ensure the security of the personal data to any persons, customers, business partners, users, stakeholders, and any other people in relation to the personal data

3. Scope

3.1 Announcement No. L&C 11/2562 on Data Privacy Policy is no longer applied. This announcement becomes effective.

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

3.3 This announcement applies to all of the Company's activities and operations in relation to the personal data.

4. Definitions

"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
“Person with Lack of Ability”	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

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. 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

5) Rights of Data Subject

6) Impacts in case that the Personal Data are not provided for compliance with a law or a contract

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, 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.

5.2 Collection of Personal Data of Person with Lack of Ability

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 Collection 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 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. 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 B.E. 2562 (2019).

7.1 Data Controller

7.1.1 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

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

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

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

7.1.5 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, and collection, usage or disclosure of Personal Data is processed in accordance with this policy and the Personal Data Protection Act B.E. 2562 (2019).

7.2 Data Processor

7.2.1 To process collection, usage or disclosure of Personal Data by order of the Data Controller

7.2.2 To set up appropriate security measures

7.2.3 To process and keep records of Personal Data processing activities

7.3 Data Protection Officer

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

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

7.3.3 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

7.4 Corporate Legal & Compliance Office

7.4.1 To establish and review the Company's Data Privacy Policy including guidelines in compliance with the law

7.4.2 To give legal consultation about the personal data protection law

7.4.3 To oversee any business units of the Company, subsidiaries and business partners to ensure their performance in accordance with the Company's Data Privacy Policy and guidelines

7.4.4 To report performance of any business units of the Company, subsidiaries and business partners to the Executive Committee

7.5 Risk Management Office

7.5.1 To assess risks and risk management plan of the Company's Personal Data processing

7.5.2 To report risk management to the Executive Committee

7.6 Internal Audit Office

7.6.1 To audit performance of persons involved with Personal Data processing

7.6.2 To verify and assess the efficiency of Personal Data Security System

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

7.7 Subsidiaries, Office Level or Equivalent

7.7.1 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).

7.7.2 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 B.E. 2562 (2019) and also notified to Corporate Legal & Compliance Office.

8. Security

To ensure the personal data privacy and security, the Company establishes the measures as follows;

8.1 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 IT Policy.

8.2 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.

8.3 In case of violation of the Company's security measures which may cause a Personal Data breach, the Company shall notify an incident to Office of the Personal Data Protection Commission within 72 hours after having become aware of it. 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.

9. 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 B.E. 2562 (2019).

10. Complaint and Misconduct Report

If it is suspected or believed that a personal data breach has occurred, complaint or misconduct report based on the rights of the Data Subject in accordance with this policy or the Personal Data Protection Act B.E. 2562 (2019) can be notified to the Company as following contact details;

CP ALL Public Company Limited

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

Email Address: DPO@cpall.co.th

Call Center: 0-2826-7744

11. 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.

12. Policy Review

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

13. Punishment

In case that he Data Controller, the Data Processor or any responsible persons relating to the Personal Data neglects, ignores, fails to conduct or command, or conducts any actions which cause violation of the Data Privacy Policy and guidelines and/or the Personal Data Protection Act B.E. 2562 (2019) and cause an offense and/or damage, he shall be punished in accordance with measures in the Company's disciplinary punishment and the law. In case that such offense causes damage to the Company and/or any other Persons, the Company may consider additional prosecution action.

This new policy will be effective from 1 November 2020 onwards.

Announced on 15 October 2019.