Personal Data Protection Policy

Alpha Capital Partners Group Public Company Limited

1. Objective

It is Alpha Capital Partners Group Public Company Limited (the "**Company**")'s policy to comply with all applicable personal data protection regulations and laws. This Personal Data Protection Policy (the "**Policy**") provides guidance to the Company's employees, as well as other related persons, with regards to our regulatory obligations. It sets the minimum required standard procedures to be undertaken to avoid breaching the Personal Data Protection Act B.E. 2562 (the "PDPA") as well as other applicable laws concerning data (together the "**Laws**") which could cause significant damages to the Company.

2. Definitions

Abbreviation/ Terminology	Description
Personal Data	any information pertaining to a person which enables the identification of such person, whether directly or indirectly, but does not include data of deceased persons;
Sensitive Data	personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, data concerning a natural person's sex life, criminal records, data concerning health, disabilities, trade union memberships, genetic data, biometric data or other data which may affect the Data Subject in the same manner as prescribed by the Personal Data Protection Committee;
Data Controller	a natural person or legal entity which has the power and responsibility to make decisions regarding the collection, use, and disclosure of Personal Data;
Data Processor	a natural person or legal entity which proceeds with the collection, use or disclosure of Personal Data as instructed by or on behalf of the Data Controller, where such person or entity is not the Data Controller;
Data Subject	a person who can be identified directly or indirectly through his/her personal data;

Abbreviation/ Terminology	Description
Data Protection Officer	any persons designated by the Company to advise obligations, monitor compliance, coordinate, and cooperate with the Office of the Personal Data Protection Committee pursuant to the PDPA.

3. Scope

This Policy applies to directors, executives, and employees of the Company, who should familiarize themselves with its terms and concepts. Failure to comply may lead to disciplinary action for misconduct, up to and including dismissal.

Where applicable, this Policy also applies to outsource vendors or other persons who collect, use or disclose Personal Data on behalf of or in the name of the Company. In the event that such persons fail to comply with this Policy, the Company may consider canceling their representation, terminating their contracts, or taking other actions as appropriate.

4. Collection, Use and Disclosure of Personal Data

The Company shall ensure that the objectives, scope, and methods used in collecting Personal Data are lawful and in compliance with the PDPA and the Laws. Personal Data shall be collected only to the extent necessary to meet the objectives for business operations and shall be used and disclosed according to the purposes notified to the Data Subjects only.

The Company shall not collect Personal Data from any other sources, apart from the Data Subject directly, except where explicitly permitted by law, and it must comply with the procedures under the PDPA.

The Company shall not collect, use or disclose Personal Data without the consent of the Data Subject unless consent is not required under the PDPA, for example, when it is necessary for the performance of a contract to which the Data Subject is a party, or when it is necessary for the legitimate interests of the Company, except where such interests are overridden by the fundamental rights of the Data Subject. Extra care and attention are required in the event that the Company collect Sensitive Data.

Requests for consent shall be made explicitly in writing or through electronic means, unless such consent cannot be provided in such forms due to its nature, in which case, consent may be obtained through verbal or other means. Requests for consent must be presented in a manner which is clearly distinguished from other messages or matters in a form that is easily accessible and understandable,

must use clear and plain language that is easily understandable, and must not be deceptive or misleading to the individual with respect to such purpose.

Consent must be freely given by an individual without fraud, harassment or misconception, and the granting of consent by an individual cannot be a condition to entering into a contract with the Company.

5. Privacy Notice

The Company, as Data Controller, is required to inform a Data Subject at the time of, or prior to, collecting Personal Data as to the purposes and reasons for the Data Subject to provide Personal Data, the types of Personal Data to be collected, retention period, type of third party persons or entities that the Personal Data may be disclosed to, Data Subject's rights, and contact details of the Company and its Data Protection Officer. This is unless the Data Subject is already aware of such information.

In order to address this requirement, the Company has issued a Privacy Notice to all relevant Data Subjects, e.g., borrowers, customers, employees, and outsource vendors. Access to the Privacy Notice is via Company's website and/or as an attachment to relevant contracts and forms.

6. Non-Disclosure Agreement and Data Processing Agreement

In the event that the Company discloses or shares Personal Data to other Data Controllers, they shall prepare non-disclosure agreements or data sharing agreements with other Data Controllers as necessary in order to prevent unauthorized or unlawful use and disclosure of such Personal Data.

In the event that the Company discloses or shares Personal Data to Data Processors, they shall prepare data processing agreements to ensure that the activities carried out by the Data Processors are in accordance with the Data Processors' obligations to ensure compliance with the PDPA.

7. Cross Border Data Transfer

The Company shall ensure that, in the event that it sends or transfers Personal Data to a foreign country, the destination country or international organization that receives such Personal Data shall have in place adequate data protection standards as determined by the Personal Data Protection Committee. This is unless one or more exemptions under the PDPA applies, for example, where the consent of the Data Subject has been obtained, provided that the Data Subject has been informed of the inadequate Personal Data protection standards of the destination country; or where it is necessary for the performance of a contract to which the Data Subject is a party or which is for the best interests of the Data Subject.

8. List of Processing Activities

The Company shall keep a record of processing activities available for Data Subjects and the Personal Data Protection Office to examine or review. The record shall include at least the followings:

- Personal Data collected,
- purpose of collection,
- details of the Data Controller (the Company and/or its subsidiaries)
- data retention period,
- authorization and conditions of access to the data,
- use and disclosure of the data,
- rejection(s) of Data Subject's request for rights
- explanation of security measures implemented in order to ensure safekeeping of the Personal Data which shall comply with minimum standards as required by law.

The Company shall ensure that the Personal Data it holds is accurate, up to date, complete and not misleading in any way.

9. Record Retention

Good record retention practices and disposal of records are essential to the Company's commitment to personal data protection. Employees are required to follow the Record Retention Policy and relevant guidelines and consistently perform required tasks.

10. Data Subject Rights

Data Subjects are entitled to these rights under PDPA:

- Right to withdraw consent
- Right to access and obtain a copy of his or her personal data for which the data controller is responsible. The Data Subject is also entitled to know the source of information that is obtained without his or her consent.
- Right to correct and/or modify data
- Right to request the controller to erase or destroy data or make it unidentifiable
- Right to restrict the use of Personal Data
- Right to receive Personal Data concerning him or her in a structured, commonly used and machine-readable format, if the Data Controller has made data in such form
- Right to object to the collection, use, or disclosure of his or her Personal Data

The Company shall always collect, use and disclose Personal Data taking into account the above rights of the Data Subject.

11. Data Protection Officer

The Data Protection Officer, with support from his or her team, will be responsible for coordinating and cooperating with, and reporting to, the Office of Personal Data Protection Committee as may be necessary; overseeing the relevant Data Protection processes and procedures to ensure they are in line with the PDPA; advising relevant parties of their rights and obligations under PDPA; as well as to perform any other tasks required.

All employees of the Company, as well as other persons who collect, use or disclose Personal Data on behalf of or in the name of the Company, shall cooperate with the Data Protection Officer.

12. Security Measures

The Company shall put in place appropriate security measures in order to prevent any unauthorized or unlawful loss, breach, access to, use, alteration, correction or disclosure of Personal Data. Such measures shall be reviewed as and when it is necessary or when the technology has changed in order to efficiently maintain appropriate security and safety measures. Such measures shall also be in accordance with the minimum standards announced by the Personal Data Protection Committee.

13. Personal Data Breach Notification

A Personal Data breach is an unauthorized or wrongful breach of data security measures causing loss, access to, change, alteration or disclosure of Personal Data, regardless whether it is intentional or due to negligence. This includes any wrongful offence relating to computer crime, cyber security threats, accidents or other incidents.

The Company shall notify the Office of the Personal Data Protection Committee of any Personal Data breach without delay and, where feasible, within 72 hours after having become aware of it, unless such Personal Data breach is unlikely to result in a risk to the rights and freedoms of a Data Subject.

If the Personal Data breach is likely to result in a high risk to the rights and freedoms of a Data Subject, the Company shall also notify the Personal Data breach and the remedial measures to the Data Subject without delay. Employees shall report a data breach to Data Protection Officer promptly, within 24 hours of becoming aware of such breach.

The procedures for Personal Data breach notification and exemptions shall be in accordance with the relevant notification of the Personal Data Protection Committee.

14. Contact Channels

1) Via Post

   Contact: Data Protection Officer

   Address: Alpha Capital Partners Group Public Company Limited

   21st Floor, Capital Tower, All Seasons Place, 87/1 Wireless Road, Lumpini, Pathumwan, Bangkok 10330, Thailand

2) Via Email

   Contact: Data Protection Officer

   Address: DataProtectionOfficer@acpg.co.th

3) Via Phone

   Telephone number: +66 2781 6030, +66 2781 6049

The Board of Directors considered and approved this Personal Data Protection Policy in the Board of Directors meeting No. 5/2023, which was held on 12 May 2023. The Policy shall come into force as from 12 May 2023.

It is the intention of the Board of Directors to review and update this policy every two years, or when there are material changes in the law. The Chief Executive Officer will be responsible for implementing this policy and ensuring the Company's compliance therewith.

(Mr. Christopher Michael Nacson)

Chairman of the Board of Directors

Alpha Capital Partners Group Company Limited