บริษัท ปูนซีเมนต์เอเชีย จำกัด (มหาชน)
Asia Cement
Public Company Limited

Personal Data Protection Policy (PDPA Policy)

Scope:	Asia Cement Public Company Limited and its affiliated companies
Author:	Legal and Compliance Department
Approved by:	Mr. Salvatore Palazzo and Mr. Nopadol Ramyarupa / Managing Directors
Date:	30 October 2026
Version:	2.0

Table of Contents

1. Introduction 1
2. Objectives and Commitment of the Company 1
3. Definitions 2
4. Governance Structure and Responsibilities 3
5. Personal Data Collected and Categories of Data Subjectsล 3
6. Legal Bases for Collection, Use or Disclosure of Personal Data 5
7. Consent Management 6
8. Rights of Data Subjects 6
9. Data Retention 7
10. Security Measures 7
11. Data Breach Response 7
12. Privacy Risk Assessment / DPIA 8
13. Cross-Border Data Transfer 8
14. Policy Review 8
15. Contact Channel for Personal Data Protection Matters 8
16. Version History 9

1. Introduction

This Personal Data Protection Policy (the "Policy") applies to Asia Cement Public Company Limited and its affiliated companies, namely Asia Cement Products Company Limited, Jalaprathan Cement Public Company Limited, Asia Cement Energy Conservation Company Limited, and Jalaprathan Concrete Company Limited (collectively, the "Company"). It sets out the principles, practices and responsibilities for the collection, use and disclosure of the personal data of employees, job applicants, customers, business partners, contractors, visitors and other relevant persons, in compliance with the Personal Data Protection Act B.E. 2562 (2019) and other applicable laws. The details of collection, use and disclosure that must be communicated to data subjects shall be set out in the privacy notices issued separately by the Company.

2. Objectives and Commitment of the Company

2.1 Rationale

Technological advances have made it easy to collect, use and disclose personal data, and any breach may cause damage to data subjects. As a data controller, the Company has therefore established this Policy to ensure that its operations comply with the law and that the rights of data subjects are adequately protected.

2.2 Seven Core Principles

The Company and all employees shall adhere to the following core principles in the collection, use and disclosure of personal data:

(1) Lawfulness, Fairness and Transparency – personal data shall be collected, used or disclosed only on a lawful basis, in a fair manner, and with clear notice to the data subject.

(2) Purpose Limitation – personal data shall be used only for the purposes notified.

(3) Data Minimization – only personal data necessary for the purposes shall be collected.

(4) Accuracy – personal data shall be kept accurate, up to date and not misleading.

(5) Storage Limitation – personal data shall not be retained for longer than necessary.

(6) Security – appropriate safeguards shall be in place to protect personal data.

(7) Accountability – the Company shall be able to demonstrate compliance with the above principles.

3. Definitions

"Processing of Personal Data" means any operation performed on personal data, including collection, recording, organization, storage, adaptation, alteration, retrieval, use, disclosure, transmission, dissemination, arrangement, combination, restriction, erasure or destruction.

"Personal Data" means any information relating to a natural person which enables that person to be identified, whether directly or indirectly, such as name and surname, national identification number, telephone number, email address, address, IP address, photographs or videos from which a person can be identified (e.g. CCTV footage), location data (GPS), and cookies that can identify a person.

"Sensitive Data" means personal data relating to race, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or any other data which may affect the data subject in a similar manner. Examples in the Company's context include health check results, medical records, fingerprint or facial scan data used for access to the Company's premises, criminal records obtained from pre-employment background checks, and trade union information.

"Data Controller" means a natural or juristic person having the power and duty to make decisions regarding the collection, use or disclosure of personal data.

"Data Processor" means a natural or juristic person who collects, uses or discloses personal data on the instructions of, or on behalf of, a Data Controller.

"Data Subject" means the natural person to whom the personal data relates, such as employees, job applicants, customers, business partners, contractors, visitors and participants in the Company's activities.

"Privacy Lead" means the person appointed by the Company to oversee, advise on and coordinate personal data protection matters within the organization, as set out in Section 4 of this Policy.

"Personal Data Breach" means an incident in which personal data is lost, or is accessed, used, altered, modified or disclosed without authority or unlawfully.

4. Governance Structure and Responsibilities

4.1 Privacy Lead

The Company shall appoint a Privacy Lead, whose duties are as follows:

(1) to advise departments on compliance with this Policy and applicable laws;

(2) to monitor compliance with this Policy and related internal processes;

(3) to coordinate on issues or queries relating to the collection, use or disclosure of personal data;

(4) to act as the main point of contact in the event of a personal data breach or complaint; and

(5) to review and update this Policy and related documents periodically.

4.2 Departmental Data Owner

The Departmental Data Owner shall ensure that the collection, use and disclosure of personal data under the responsibility of their department comply with this Policy, and shall coordinate with the Privacy Lead as appropriate.

4.3 Duties of Employees

All employees shall comply with this Policy, access and use personal data only to the extent necessary for the performance of their duties, and immediately report any breach or suspected data security incident to the Privacy Lead or their supervisor. Non-compliance with this Policy may result in disciplinary action in accordance with the Company's work rules.

5. Personal Data Collected and Categories of Data Subjectsล

The Company collects, uses and/or discloses the personal data of the following main categories of data subjects. Details for each category are set out in the relevant privacy notice.

5.1 Employees and Job Applicants

Data Category	Examples
Internally Disclosed Data	Name and surname, employee ID, department, position, employment status, company email address, work mobile phone number
Basic Data	Name, address, age, date of birth, gender, telephone number, email address, front-facing photograph, nationality, marital status, military service status (for male employees)

Data Category	Examples
Compensation Data	Annual and monthly income, salary and bonus, bank account details, check numbers, debit/credit cards, financial transaction history, withholding tax
Human Resources Data	Performance evaluations, educational background, qualifications/licenses, visas and work permits (for foreign nationals), work experience, disciplinary actions/commendations, training records, benefits and welfare, social security data, provident fund, personal income tax
Family and Relatives Data	Family structure, dependents, emergency contact details

Sensitive Data of this category includes race, religion, health conditions, medical records, physical or mental impairments, health check results, criminal records from pre-employment background checks, and biometric data such as fingerprints or facial scans used for access to the Company's premises. The collection, use or disclosure of such data shall be subject to Section 6.2.

5.2 Customers, Business Partners and Contractors

Contact details (name, address, telephone number and email address), account and financial transaction data, quotation and contract data, and data of directors or representatives of corporate customers or business partners.

5.3 Visitors

CCTV footage and data from registration or the exchange of identification cards before entering the premises (as detailed in the Company's CCTV Privacy Notice).

5.4 Website Users and Marketing Event Participants

Website browsing data, cookies, and photographs or videos recorded at events or in the Company's marketing communications.

5.5 Directors, Shareholders and Corporate Representatives

As a public limited company, the Company may collect, use and/or disclose the personal data of its directors, shareholders and representatives of corporate customers or business partners in order to comply with laws applicable to public limited companies and for corporate governance purposes.

6. Legal Bases for Collection, Use or Disclosure of Personal Data

6.1 General Principles

The Company shall collect, use or disclose personal data only where there is a legal basis to do so, and shall identify the appropriate legal basis for each activity before it begins. The legal bases on which the Company may rely are as follows:

(1) Legal Obligation

Where the Company is required to comply with a legal obligation, such as under labor law, tax law or laws applicable to public limited companies.

(2) Vital Interests

Where necessary to prevent or suppress a danger to a person's life, body or health.

(3) Contract

Where the data subject is a party to a contract with the Company, or where necessary to take steps at the data subject's request prior to entering into a contract, such as an employment contract or a sale and purchase contract.

(4) Public Interest

Where necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company.

(5) Legitimate Interest

Where necessary for the legitimate interests of the Company or another person, provided that such interests do not override the fundamental rights of the data subject, such as the use of CCTV for security purposes.

(6) Historical Archives, Research or Statistics

Where necessary for the preparation of historical documents or archives in the public interest, or for purposes relating to research or statistics.

(7) Consent

Where the data subject has consented to the collection, use or disclosure of their personal data for the notified purposes, such as sending marketing communications or using photographs for public relations purposes.

6.2 Legal Basis for Sensitive Data

The collection, use or disclosure of Sensitive Data requires the explicit consent of the data subject, unless a legal exception applies, such as to prevent a danger to life where the data subject is incapable of giving consent, to establish or exercise legal claims, or to comply with laws relating to

medicine, public health or labor protection. The Company shall restrict access to Sensitive Data to persons with relevant duties and shall implement security measures in accordance with Section 10.

7. Consent Management

7.1 Requirements for Valid Consent

Where the Company relies on consent as the basis for processing personal data, the Company shall obtain explicit consent, clearly inform the data subject of the purposes of the collection, use or disclosure, present the request separately from other matters, and use language that is easy to understand. The Company shall not require the data subject to give consent beyond what is necessary for the relevant purpose or service.

7.2 Withdrawal of Consent

Data subjects may withdraw their consent at any time, in the same or a similar manner to that in which it was given, unless restricted by law or contract. The Company shall inform the data subject of the consequences of withdrawal (if any) before acting on the request.

7.3 Minors, Incompetent Persons and Quasi-Incompetent Persons

Consent shall be obtained as follows:

(1) Minors: consent shall be obtained from the person exercising parental power, subject to the conditions prescribed by law.

(2) Incompetent persons: consent shall be obtained from the guardian.

(3) Quasi-incompetent persons: consent shall be obtained from the curator.

8. Rights of Data Subjects

The Company respects the legal rights of data subjects and shall consider requests to exercise such rights submitted through the channel set out in Section 15. Data subjects, or persons authorized to act on their behalf under Section 7.3, may exercise the following rights:

(1) the right to access and obtain a copy of their personal data, or to request disclosure of the source of personal data obtained without their consent;

(2) the right to receive or transfer their personal data (data portability) where the data is in a machine-readable format;

(3) the right to object to the collection, use or disclosure of their personal data;

(4) the right to request the erasure or destruction of their personal data, or its anonymization;

(5) the right to request the restriction of use of their personal data;

(6) the right to request the rectification of their personal data so that it is accurate, up to date and not misleading;

(7) the right to withdraw consent; and

(8) the right to lodge a complaint with the Expert Committee where the Company or its data processor violates or fails to comply with personal data protection law.

9. Data Retention

The Company shall retain personal data only for as long as necessary to achieve the purposes of its collection, use or disclosure, or for the period prescribed by law. In general, personal data shall be retained for no longer than 10 years, unless a longer period is required or permitted by law. Upon expiry of the retention period, or when the processing of the personal data is no longer necessary, the Company shall erase, destroy or anonymize the data as appropriate. The Company may, however, continue to retain personal data where there are lawful grounds to do so.

10. Security Measures

The Company shall implement appropriate security measures to prevent the loss of, and unauthorized or unlawful access to, use, alteration or disclosure of, personal data, and shall review or update such measures as necessary or when relevant technologies or risks change. Where the Company engages an external service provider to process personal data on its behalf, the Company shall set out the service provider's obligations regarding confidentiality and data security in the relevant contract or agreement.

11. Data Breach Response

The Company shall ensure that personal data breaches are reported and managed appropriately in order to limit their impact and prevent recurrence. Personal data breaches may include sending data to the wrong recipient, loss of documents or devices, cyber-attacks, data leaks from external service providers, unauthorized removal of data, or inappropriate access rights.

Any person who discovers a breach shall report it immediately through the channel designated by the Company so that the risk can be assessed, the damage contained and remedied, the incident recorded, and preventive measures reviewed. Where a breach is likely to affect the rights and freedoms of data subjects, the Company shall notify the Office of the Personal Data Protection Committee without delay and within 72 hours of becoming aware of it. Where the risk is high, the Company shall also notify the affected data subjects of the breach and the remedial measures without delay.

12. Privacy Risk Assessment / DPIA

Processing activities that pose a high risk to the rights and freedoms of data subjects, such as activities involving biometric data, the monitoring of behavior or location, the use of artificial intelligence (AI), or other activities with similar risks, shall be subject to a Privacy Risk Assessment / DPIA before they commence. The Departmental Data Owner shall prepare the assessment and submit it to the Privacy Lead for review.

13. Cross-Border Data Transfer

The Company may send or transfer personal data abroad only where the destination country or international organization has adequate personal data protection standards, where the Company has put in place appropriate safeguards as required by law, or where a legal exception applies, such as where the data subject has given consent, where the transfer is necessary to comply with the law or to perform a contract, for the benefit of the data subject, to prevent a danger to life, body or health, or for important public interest purposes.

14. Policy Review

The Legal and Compliance Department is responsible for reviewing this Policy at least once a year, or upon any material change in applicable laws or in the Company's personal data processing activities, and for proposing amendments to the Managing Directors for approval.

This Policy shall come into effect on 30 October 2026.

15. Contact Channel for Personal Data Protection Matters

The Company designates LegalandCompliance@acc.co.th as the central channel for exercising data subject rights, making enquiries, and reporting incidents or lodging complaints relating to personal data protection. The Company shall respond to requests or enquiries within 7 business days, or no later than 14 business days, as the case may be, and shall act on requests to exercise data subject rights within the period prescribed by law.

16. Version History

Date	Version	Author	Description of Changes
June 2022	1.0	Legal Department	Initial Issue
October 2026	2.0	Legal Department	Revised Policy

Approved by: Managing Directors

Salvatore Palazzo

(Mr. Salvatore Palazzo) (Mr. Nopadol Ramyarupa)