



DATA PROTECTION POLICY FOR BUSINESS COUNTERPARTIES

POLICY

SG-LE-POL-006

REVISION: 1.0

Approved By: Zhi Lim

Created By: Charmian Ong



Policy

DATA PROTECTION POLICY FOR BUSINESS COUNTERPARTIES

Revision: 1.0


Number: SG-LE-POL-006

Release Date: 18-May-26

THIS DOCUMENT AND THE INFORMATION CONTAINED HEREIN IS CONFIDENTIAL AND PROPRIETARY. FOR INTERNAL USE ONLY.

REVISION INDEX

Revision	Date	Description of Changes	Revised By
1.0	18 May 26	Initial Release	Zhi Lim

	Policy		
	DATA PROTECTION POLICY FOR BUSINESS COUNTERPARTIES		
	Revision: 1.0	Number: SG-LE-POL-006	Release Date: 18-May-26
THIS DOCUMENT AND THE INFORMATION CONTAINED HEREIN IS CONFIDENTIAL AND PROPRIETARY. FOR INTERNAL USE ONLY.			

1.0 INTRODUCTION AND SCOPE


- 1.1 This Data Protection Notice (“**Notice**”) sets out the basis upon which BE C&I Solutions Holding Pte Ltd and its affiliates and subsidiaries (collectively, “**BECIS**”, “**we**”, “**us**”, or “**our**”) collect, use, disclose, store, transfer, or otherwise process personal data of our business counterparties.
- 1.2 This Notice is designed to comply with the Singapore Personal Data Protection Act 2012 (No. 26 of 2012), as amended, re-enacted, or replaced from time to time (the “**PDPA**”), and with other applicable data protection and privacy laws in jurisdictions in which BECIS operates, including but not limited to Malaysia, Thailand, the Philippines, India, China, Cambodia, and Vietnam. Where any provision of this Notice conflicts with mandatory requirements of applicable local law, the local law shall prevail to the extent of the inconsistency.
- 1.3 This Notice applies to personal data in our possession or under our control, including personal data held by third-party service providers engaged by us to process personal data on our behalf.

2.0 DEFINITIONS

- 2.1 “**Business Counterparty**” means any individual, or any individual acting on behalf of an entity, who: (a) has contacted us through any means to enquire about our goods or services; (b) has entered or may enter into a contract with us for the supply of goods or services by us or to us; or (c) otherwise engages with us in a business capacity, including but not limited to customers, suppliers, vendors, service providers, consultants, agents, and their respective representatives, authorised signatories, directors, and beneficial owners (each a “Counterparty”).
- 2.2 “**Entity data**” means information relating to a corporate or other legal entity (such as business profiles, corporate registration documents, financial statements, and organisational charts). To the extent that entity data incidentally contains personal data of identifiable individuals (for example, director names, signatory details, or shareholder information), such personal data will be processed in accordance with this Notice.
- 2.3 “**PDPC**” means the Personal Data Protection Commission of Singapore, or its successor body.
- 2.4 “**Personal data**” means any data, whether true or not, about an individual who can be identified: (a) from that data alone; or (b) from that data in combination with other information to which we have or are likely to have access, and includes any equivalent concept under applicable local law.
- 2.5 “**Processing**” means any operation performed on personal data, including collection, recording, organisation, storage, adaptation, alteration, retrieval, use, disclosure, transfer, erasure, or destruction.
- 2.6 Other terms used in this Notice shall have the meanings given to them in the PDPA or applicable local law (where the context so permits).

3.0 CATEGORIES OF PERSONAL DATA COLLECTED

- 3.1 Depending on the nature of your interaction with us, we may collect and process the following categories of personal data (this list is non-exhaustive):
 - a. **Identity and biographical data:** name, gender, date of birth, nationality, NRIC/FIN, passport number, or equivalent national identification number;
 - b. **Contact data:** address, email address, telephone number, and other contact details;

	Policy		
	DATA PROTECTION POLICY FOR BUSINESS COUNTERPARTIES		
	Revision: 1.0	Number: SG-LE-POL-006	Release Date: 18-May-26
THIS DOCUMENT AND THE INFORMATION CONTAINED HEREIN IS CONFIDENTIAL AND PROPRIETARY. FOR INTERNAL USE ONLY.			


- c. **Professional and employment data:** job title, employer name, department, professional qualifications, and business role;
- d. **Financial and transactional data:** bank account information, payment details, credit-related information, and transaction records;
- e. **Due diligence data:** information collected in connection with know-your-customer (KYC), anti-bribery and anti-corruption (ABAC), sanctions screening, and counterparty risk assessment processes, including information about directors, shareholders, beneficial owners, and authorised signatories contained in corporate documents;
- f. **Contractual data:** information provided in the course of negotiating, executing, or performing a contract with us; and
- g. **Visual and audio data:** photographs and other audio-visual information.

4.0 PURPOSE OF COLLECTION, USE AND DISCLOSURE

4.1 We may collect, use, and disclose your personal data for the following purposes:

- a. **Contractual performance:** performing obligations in the course of or in connection with our provision or receipt of goods and/or services;
- b. **Identity verification and due diligence:** verifying your identity and conducting KYC, ABAC, sanctions screening, counterparty risk assessment, and other due diligence checks required or prudent in the context of our business relationships;
- c. **Relationship management:** responding to, handling, and processing queries, requests, applications, complaints, and feedback; and managing our ongoing business relationship with you;
- d. **Financial processing:** processing payments, invoices, credit assessments, and related financial transactions;
- e. **Marketing and business communications:** sending you information about our goods, services, industry developments, events, and initiatives (subject to your right to opt out at any time – see clause 6.4);
- f. **Legal and regulatory compliance:** complying with applicable laws, regulations, codes of practice, guidelines, court orders, or regulatory directions in any relevant jurisdiction, and assisting in law enforcement or regulatory investigations;
- g. **Corporate transactions:** facilitating any proposed or confirmed merger, acquisition, divestiture, business asset transaction, or corporate restructuring involving any BECIS entity;
- h. **Dispute resolution:** establishing, exercising, or defending legal claims and managing disputes;
- i. **Disclosure to third parties:** transmitting personal data to our third-party service providers, agents, professional advisers, and relevant governmental and regulatory authorities (whether in Singapore or abroad) for the purposes set out above; and
- j. **Incidental purposes:** any other purposes directly related to or in connection with the above.

4.2 We may disclose your personal data: (a) where required for the purposes set out in clause 4.1; or (b) to third-party service providers, agents, and other organisations engaged by us to perform any of the functions listed above on our behalf.

	Policy		
	DATA PROTECTION POLICY FOR BUSINESS COUNTERPARTIES		
	Revision: 1.0	Number: SG-LE-POL-006	Release Date: 18-May-26
THIS DOCUMENT AND THE INFORMATION CONTAINED HEREIN IS CONFIDENTIAL AND PROPRIETARY. FOR INTERNAL USE ONLY.			

4.3 The purposes listed above may continue to apply after our relationship with you has ended, for a reasonable period necessary to fulfil those purposes or as required by law (including to enforce our rights under any contract with you or to comply with record-keeping and regulatory obligations).

5.0 CONSENT

5.1 We generally collect your personal data on the basis of: (a) your consent; (b) the necessity of processing for the performance of a contract to which you are a party or for pre-contractual steps taken at your request; or (c) as permitted or required by applicable law without consent.

5.2 Where we rely on consent, we will ensure you have been notified of the purposes for which the data is collected before or at the time of collection, and that your consent is given voluntarily. Consent may be provided by you directly or via a third party duly authorised by you to disclose your personal data to us (your “**authorised representative**”).

6.0 WITHDRAWAL OF CONSENT

6.1 You may withdraw your consent for the collection, use, or disclosure of your personal data at any time by submitting a written request to the Data Protection Officer at the contact details provided in clause 13.

6.2 Upon receiving your request, we will process it within a reasonable time (and in any event within ten (10) business days of receipt) and notify you of the consequences of the withdrawal, including any impact on our ability to continue providing or receiving goods or services.

6.3 Withdrawal of consent does not affect the lawfulness of processing carried out prior to the withdrawal, and does not affect our right to continue processing personal data where such processing is permitted or required by law without consent.

6.4 **Marketing opt-out.** You may opt out of receiving marketing communications from us at any time by contacting the Data Protection Officer or using the unsubscribe mechanism included in any marketing communication. We will give effect to your opt-out request within a reasonable time.


7.0 ACCESS TO AND CORRECTION OF PERSONAL DATA

7.1 You may request: (a) access to a copy of the personal data we hold about you, or information about how we use or disclose your personal data; or (b) correction or updating of any personal data we hold about you, by submitting a written request to the Data Protection Officer.

7.2 A reasonable fee may be charged for an access request to the extent permitted by applicable local law. If so, we will inform you of the fee before processing your request.

7.3 We will respond to your request as soon as reasonably possible. If we are unable to respond within thirty (30) days of receiving your request, we will inform you in writing within that period of the time by which we expect to respond.

7.4 If we are unable to provide the requested personal data or to make a requested correction, we will inform you of the reasons (except where we are not required to do so under applicable law).

	Policy		
	DATA PROTECTION POLICY FOR BUSINESS COUNTERPARTIES		
Revision: 1.0	Number: SG-LE-POL-006	Release Date: 18-May-26	
THIS DOCUMENT AND THE INFORMATION CONTAINED HEREIN IS CONFIDENTIAL AND PROPRIETARY. FOR INTERNAL USE ONLY.			

8.0 PROTECTION OF PERSONAL DATA

- 8.1 We implement appropriate administrative, physical, and technical measures to protect personal data from unauthorised access, collection, use, disclosure, copying, modification, disposal, or similar risks. These measures include, without limitation:
- access controls and authentication requirements;
 - encryption of personal data in transit and at rest;
 - up-to-date anti-malware and intrusion detection systems;
 - need-to-know restrictions on internal access; and
 - contractual obligations on third-party service providers to maintain equivalent or higher standards of protection.
- 8.2 No method of electronic transmission or storage is completely secure. While we cannot guarantee absolute security, we are committed to reviewing and enhancing our information security measures on an ongoing basis.

9.0 ACCURACY OF PERSONAL DATA


- 9.1 We rely on the personal data provided to us (or that is provided by your authorised representative). To ensure your personal data remains current, complete, and accurate, please notify the Data Protection Officer in writing of any changes.

10.0 RETENTION OF PERSONAL DATA

- 10.1 We retain personal data only for as long as necessary to fulfil the purpose for which it was collected, or as required or permitted by applicable laws.
- 10.2 As a general baseline, personal data will be retained for a maximum period of seven (7) years from the end of our business relationship with you (or such longer period as required by applicable law in the relevant jurisdiction). Different retention periods may apply to specific categories of data where required by local law or regulation.
- 10.3 Upon expiry of the applicable retention period, we will cease to retain the personal data, or remove the means by which the data can be associated with you, as soon as reasonably practicable.

11.0 CROSS-BORDER TRANSFERS OF PERSONAL DATA

- 11.1 As BECIS operates across multiple jurisdictions, we may transfer your personal data to BECIS entities or authorised third-party service providers located in countries other than the country in which it was originally collected. Such transfers may be necessary for:
- the performance of a contract with you;
 - pre-contractual steps taken at your request;
 - centralised compliance, due diligence, and governance functions;
 - group financial reporting, audit, and corporate transactions; or
 - any other purpose identified in clause 4 of this Notice.
- 11.2 Where your consent is required under applicable local law for a cross-border transfer, we will obtain such consent before the transfer takes place.
- 11.3 In all cases, we will take appropriate measures to ensure that your personal data receives a standard of protection at least comparable to that provided under the PDPA (or the

	Policy		
	DATA PROTECTION POLICY FOR BUSINESS COUNTERPARTIES		
	Revision: 1.0	Number: SG-LE-POL-006	Release Date: 18-May-26
THIS DOCUMENT AND THE INFORMATION CONTAINED HEREIN IS CONFIDENTIAL AND PROPRIETARY. FOR INTERNAL USE ONLY.			

applicable local law, whichever sets the higher standard), including by implementing appropriate contractual safeguards.

12.0 DATA BREACH NOTIFICATION

12.1 In the event of a data breach that is assessed to be notifiable under the PDPA (or applicable local law), BECIS will notify the PDPC (or the relevant local data protection authority) within three (3) calendar days of confirming the breach is notifiable, or within such other timeframe as required by applicable local law.

12.2 Where required by applicable law, or where BECIS determines it is appropriate, we will also notify affected individuals of the data breach and provide guidance on steps they may take to protect themselves.

13.0 DATA PROTECTION OFFICER

13.1 For any enquiries, feedback, access or correction requests, consent withdrawal requests, or marketing opt-out requests, please contact:

Name: Zhi Lim

Title: Data Protection Officer

Email: DPO@be-cis.com

14.0 AUTOMATED DECISION-MAKING

14.1 Where BECIS uses automated processing tools (including artificial intelligence or algorithmic systems) in the context of its business relationships (such as in counterparty risk assessment, sanctions screening, or credit evaluation), we will:

- a. inform affected individuals that automated processing is being used where required by applicable law;
- b. ensure that meaningful human oversight is applied before any decision with significant effect is made solely on the basis of automated processing; and
- c. provide individuals with the right to request human review of any automated decision that significantly affects them, where required by applicable law.

15.0 CHANGES TO THIS NOTICE

15.1 This Notice applies in conjunction with any other notices, contractual clauses, and consent clauses that apply in relation to the processing of your personal data by us.

15.2 We may revise this Notice from time to time. Material changes will be communicated through reasonable means. The revised Notice will take effect from the date stated on the updated version. Your continued engagement with us following such communication constitutes your acknowledgement of the revised Notice.