

Sinarmas Cepsa Singapore Personal Data Protection Policy (also known as “Privacy Policy”)

1. Introduction

- 1.1 This Personal Data Protection Policy (“Policy”) is published on 01 January 2025 (“Effective Date”).
- 1.2 This Policy sets out the basis upon which Sinarmas Cepsa Singapore¹ (“we”, “us” or “our”) may collect, use, disclose or otherwise process individuals² (“your”, “you” and “yours”) personal data responsibly and in compliance with applicable data protection related laws. Where personal data is processed in Singapore, the Singapore Personal Data Protection Act (2012) (“PDPA”) shall apply or in Indonesia, its Data Protection Rule no 27, 2022 as an example. This Policy applies to personal data in our possession or under our control, including personal data in the possession of organisations which we have engaged to collect, use, disclose or process personal data for our purposes.
- 1.3 This Policy may be updated from time to time, with amendments to the PDPA or to provide you with additional information. We strongly encourage you to read this Policy.

2. Personal Data

- 2.1 For purposes of this Policy, Personal Data means any information or combination of information, relating, directly or indirectly to an identified or identifiable natural person.
- 2.2 Depending on the nature of your interaction with us, the Personal Data we collect may include your personal identification information, business information, health and medical information, account and profile information, network traffic and related data and/or any other information which have been provided to us or we may have access to, in the course of your interaction with us.
- 2.3 For more details on Personal Data which may be collected, please refer to Appendix 1.

3. How do we collect Personal Data?

We generally collect Personal Data that (a) you knowingly and voluntarily provide in the course of or in connection with your interaction with us, or via a third party who has been duly authorised by you to disclose your personal data to us (your “authorised representative”), after (i) you (or your authorised representative) have

been notified of the purposes for which the data is collected, and (ii) you (or your authorised representative) have provided written consent to the collection and usage of your Personal Data for those purposes, or (b) collection and use of Personal Data without consent is permitted or required by the PDPA or other applicable laws. We shall seek your consent before collecting any additional Personal Data and before using your personal data for a purpose which has not been notified to you (except where permitted or authorised by law).

4. For which purpose is Personal Data collected?

Personal Data shall be collected, used, transferred or otherwise processed in accordance with the PDPA, for one or more of the following purposes:

- 4.1 Business Purposes: Legitimate purposes as appropriate to conduct our business, which include the performance of contractual obligations, account management of Individuals, customer service and support, finance and accounting, research and development, internal management and control, and any other reasonably related activities.
- 4.2 Human resources and personnel management: This includes the performance of an employment contract or other contract with an employee (or to take necessary steps at the request of an employee prior to entering into a contract), or for managing the employment-at-will relationship.
- 4.3 Health, safety and security: For purposes necessary to ensure occupational safety and health, the protection of our assets, your verification and your access rights and its status;
- 4.4 Compliance with legal and regulatory obligations: For purposes necessary for the compliance with a legal obligation to which we are subject;
- 4.5 Marketing and Promotion: We may, when processing Personal Data for marketing communications and/or promotions, either:
 - a) obtain your consent; and/or
 - b) offer you opportunity to not proceed with the processing and/or to choose not to receive such communications.

If you wish to withdraw consent to receive such materials, please contact us (contact details provided below).

- 4.6 Secondary Purposes: For secondary purposes such as:

- a) transferring the Personal Data to an archive;
- b) conducting internal audits or investigations;
- c) implementing business controls;
- d) conducting statistical, historical or scientific research as required for our business operations;
- e) preparing or engaging in dispute resolution;

- f) using legal or business consulting services;
- g) managing insurance or other benefits related issues; and/or

4.7 Any other reasonably related purposes.

5. Ensuring accuracy of Personal Data

5.1 We generally rely on Personal Data provided by you. In order to ensure that your Personal Data is current, complete and accurate, please update us if there are changes to your Personal Data by informing our Data Protection Officer in writing or via email at the contact details provided below.

5.2 Furthermore, if you act as an intermediary or are supplying us with Personal Data and information relating to a third-party/other individual, please note that you need to ensure that such Personal Data is collected in compliance with the PDPA or any other applicable laws.

6. Sharing your Personal Data with others

6.1 Your Personal Data may be shared with our employees, representatives and/or Affiliates.

6.2 Access to Personal Data, will be limited to those who have a need to know the information for the purposes described in this Policy.

6.3 From time to time, we may need to share your Personal Data with external parties, which may include the following:

a) service providers, vendors, suppliers: we contract with authorised external parties or companies that provide products and services to us necessary for our operations;

b) public and governmental authorities: when required by law, or as necessary to protect our rights, we may share your Personal Data to public and governmental authorities that regulate or have jurisdiction over us;

c) professional advisors and others: we work with and receive support from certain professional advisors such as banks, insurance companies, auditors, lawyers, accountants, and payroll advisors, consultants; and/or

d) other parties in connection with corporate transactions: we may also, from time to time, share your Personal Data in the course of corporate transactions, such as during a sale of a business or a part of a business to another company, or any reorganisation, merger, joint venture, or other disposition of our business, assets, or stock.

7. Cross-border transfer of Personal Data

7.1. Due to our international presence, your Personal Data may be accessed by or transferred to our Affiliates and/or authorised external parties from various countries around the world in order for us to fulfil the purposes described in this Policy.

7.2 As a result, we may transfer your Personal Data to countries located outside of Singapore, which may have data protection related laws and rules that are different from the standards provided under the PDPA

7.3 Personal Data may be transferred to an authorised external party, located internationally only if, we believe it is necessary or appropriate to:

a) ensure compliance with applicable data protection related laws which may include responding to requests from public and government authorities, cooperation with law enforcement agencies or other legal reasons; and/or

b) satisfy purposes for which Personal Data has been collected by us or to enforce our terms and conditions.

8. When do we retain your Personal Data?

8.1 We may retain your Personal Data for as long as it is necessary to fulfil the purposes for which they were collected, or as required or permitted by applicable laws.

8.2 We will cease to retain your Personal Data, or remove the means by which the data can be associated with you, as soon as it is reasonable to assume that such retention no longer serves the purposes for which the Personal Data were collected, and are no longer necessary for legal or business purposes.

9. How do we protect your Personal Data?

9.1 To safeguard your Personal Data from unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks, we have introduced appropriate administrative, physical and technical measures such as up-to-date antivirus protection, encryption and the use of privacy filters to secure all storage and transmission of personal data by us, and disclosing personal data both internally and to our authorised third party service providers and agents only on a need-to-know basis.

9.2 You should be aware, however, that no method of transmission over the Internet or method of electronic storage is completely secure. While security cannot be guaranteed, we strive to protect the security of your information and are constantly reviewing and enhancing our information security measures.

9.3 If you have any reason to believe that your interaction with us is no longer secure, please contact us (contact details provided below).

10. How can you contact us for choices available to you?

10.1 With respect to processing of your Personal Data, upon successful verification of your identity, you may:

- a) obtain information on the processing of your Personal Data over the past one year, subject to applicable fee(s) related to the costs of processing your access request;
- b) request to update or correct your Personal Data, provided we are satisfied on reasonable grounds that such a correction should be made; and/or
- c) withdraw your consent to use of your Personal Data. Please note that your request may affect the products and services we are able to offer to you;
- d) obtain Personal Data that is in our possession and/or under our control in a commonly used machine-readable format.

10.2 If you have any inquiries, requests, feedback or complaints in relation to protecting your Personal Data, please contact the Data Protection Office via the following channels:

1. Call: +65 6715 8429
2. Email: pdpo@sinarmascepsa.com
3. Written communication mailed to: Data Protection Officer,
Sinarmas Cepsa Pte Ltd, 108 Pasir Panjang Road #05-02
Golden Agri Plaza Singapore 118535

10.3 We will do our best to respond to you within a reasonable time and no longer than 30 days from the date we receive your inquiry, request, feedback or complaint.

11. How do we respond to data breach?

11.1 In the event of data breach which will likely result in significant harm to individuals we will notify PDPC in Singapore or related Indonesian authorities and impacted individuals as soon as practicable. Definition of notifiable breach:

1. Medical or financial data
2. Data breach impacting more than 500 people

11.2 Incident response plan is in place to contain data breach to prevent further compromise, assess data breach to determine the root cause (where possible) and the effectiveness of containment actions taken, report the

incident as per 11.1, and evaluate our response to consider actions that can be taken to prevent future data breaches.

12. Updates to Policy

12.1 We may revise this Policy from time to time. Any change will become effective as on the Effective Date. You are strongly advised to review this Policy periodically for any change or update.

Appendix 1 Personal Data which may be collected (including but not limited to)

Types of Personal Data	Examples (Non-exhaustive)
Personal identification information (personal particulars, demographic and contact information)	Name, NRIC, travel and permit document (passport, employment pass, VISA details), gender, date of birth, country of birth, country of residence, nationality, citizenship, marital status, relatives (i.e. spouses, next of kin, dependents, children, and partners), race, ethnicity, religion, contact number(s), email address(es).
Financial Information	Financial Statements & other confidential financial information which may be shared in the ordinary course of business
Network traffic and other related data	Identification numbers, location data, online identifiers, IP address, cookies, web beacons, device identification details, language settings.
Compensation and payroll	Bank account information, salary, bonus, payroll deductions including direct insurance.
Job, position, and organisation data.	Department, supervisor, office address, work location, permit details, hire date, job title, designation, business unit, part-time or full time position, work history, termination date and reason, retirement eligibility, promotions and disciplinary records, date of transfers, reporting manager(s), other details of employment contract.
Performance and benefits data	Performance reviews and ratings, incentives, awards, retirement, benefits data of family members/dependents such as names and date of birth.
Tax Data	Tax number, contribution rates, tax preferences
Data resulting from internal or external communications	Contents of email, records of communication through bots, messaging tools, mobile communications.
Information that you decide to voluntarily share with us	Feedback, opinions, reviews, comments, any information you may share with us on our social media platform, internal communication platforms and websites.

¹ Sinarmas Cepssa, Singapore is a network of oleochemical companies including without limitation Sinarmas Cepssa Pte Ltd and their respective Affiliates. "Affiliates" shall mean any entity that controls, is controlled by, or is under common control, in each case either directly or indirectly with either a subsidiary or related corporation of Sinarmas Cepssa, Singapore, where "control" means the ownership of or the power to vote representing more than 50% of voting stock, shares or interests of the entity.

² "Individual" means a natural person, whether living or deceased.