

# Sovereign Management Services Pte Ltd

## Privacy Notice for provision of corporate services.

### 1. Introduction

Sovereign Management Services Pte Ltd, part of the Sovereign Group (“SMS”, “we”, “us”, “our”) is committed to protecting the privacy and security of the Personal Data we collect from clients (“you/your”). We are further committed to ensuring we meet our legal obligations in Singapore when processing your Personal Data under the relevant laws, in particular data protection. In Singapore, the relevant legal framework is set out in the Personal Data Protection Act 2012 (“PDPA”) and the supervisory authority is the Personal Data Protection Commission (“PDPC”).

SMS is a company registered in the Republic of Singapore under registration number [200405392N] and we have our registered office at 3 Phillip St, #14-05 Royal Group Building, Singapore 048693. We are the Controller (organisation) of the Personal Data we collect.

The purpose of this privacy notice is to explain what Personal Data we collect about you and how we process it in order to provide corporate services to you. This privacy notice also explains your rights, so please read it carefully. If you have any questions, you can contact us using the information provided below under the ‘How to contact us’ section.

This Privacy Notice may be updated and/ or re-issued at any time, and we will provide you with notice of any such updates via either email and/or our Website.

### 2. Personal Data we collect

Personal Data under the PDPA refers to all *'data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access'*. The PDPA expressly excludes the following categories of Personal Data from its application:

- “business contact information”, which is defined as 'an individual's name, position name or title, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes', unless expressly referred to in the PDPA; which is defined as 'an individual's name, position name or title, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes', unless expressly referred to in the PDPA;
- Personal Data that is contained in a record that has been in existence for at least 100 years; and
- Personal Data about a deceased individual who has been dead for more than ten years.

Even though there is no special category for Personal Data of a more sensitive nature (“Sensitive Personal Data”) in the PDPA, the PDPC takes the view that Sensitive Personal Data should be safeguarded by a higher level of protection.

Additionally, in the Personal Data Protection (Notification of Data Breaches) Regulations 2021 (“Breach Notification Regulations”), the PDPC prescribes a list of data that, if subject to a data breach, would be deemed to result in significant harm to individuals. These include the following broad categories of Personal Data:

- financial information which is not publicly disclosed;
- Personal Data which would lead to the identification of vulnerable individuals (e.g. leading to the identification of a minor who has been arrested for an offence);
- life, accident, and health insurance information which is not publicly disclosed;
- specified medical information, including the assessment and diagnosis of HIV infections;
- information related to adoption matters;
- private keys used to authenticate any or digitally sign an electronic record or transaction; and
- an individual's account identifier and data for access into the individual's account.

### 3. Sensitive Personal Data

As explained above, we may also collect, store, and use Sensitive Personal Data about you. For example, we may collect information about your health and medical conditions for health and safety purposes, in order to make necessary adjustments to your work environment. We may be required to ask you for equal opportunities monitoring information.

In the course of providing services to you, the Sensitive Personal Data acquired by us may include (without limitation to the following):

- an individual's national identification numbers (e.g. National Registration Identity Card and passport numbers);
- Where applicable, an individual's criminal history/records
- Personal Data of a financial nature (e.g. bank account details, Central Depository account details, securities holdings, transaction and payment summaries);
- insurance information (e.g. names of the policyholder's dependents or beneficiaries, sum insured under the insurance policy, the premium amount and type of coverage);
- an individual's personal history involving drug use and infidelity;
- sensitive medical conditions; and
- Personal Data of minors.

The Personal Data we collect about you will be the minimum necessary to provide corporate services. The type of Personal Data we collect is outlined in the table below in the section entitled ‘Purposes, lawful bases and retention periods’.

### 4. How we collect your Personal Data

SMS collects your Personal Data in a variety of ways. We generally do not collect your Personal Data unless:

- it is provided to us voluntarily by you directly 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

- collection and use of Personal Data without consent is permitted or required by the PDPA or other 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).

However, we may also need to collect Personal Data from certain third parties (including but not limited to) :

- Other Sovereign Group offices and existing clients;
- Introducers;
- Legal Firms; and
- Any other regulated institutions

## **5. Cookies**

A cookie is a small text file which is placed onto your device (e.g computer, smartphone or other electronic device) when you use our website.

Our website uses cookies. For further information about cookies and how we use them, please see Sovereign [Cookie Notice](#).

## **6. Accuracy of Personal Data**

It is important that the Personal Data we hold about you is accurate and up to date. Please keep us informed if your Personal Data changes during your working relationship with us.

## **7. Purposes, lawful bases and retention periods**

We will only use your Personal Data when the law allows. Without limitation to the following, we will commonly use your Personal Data in the following circumstances:

Categories of individuals	Types of Personal Data	Purpose of Processing	Lawful Basis	Retention Period Source: Group Baseline
Client	Name, address, email address	For purposes in relation to or ancillary to the performance of contract with SMS	Legitimate Interests pursuant to contract with SMS	(7years after terminating business relationship with the customer)
Client	Name, job title, work email address, work phone number, company you work for, social media accounts	To sent you marketing newsletters and other promotional material	Consent by you or your authorised representative	(7years after terminating business relationship with the customer)
Third Parties	Name, job title, work email address, work phone number, company you work for	Supplier / Consultant payments	Legitimate Interests pursuant to contract with SMS	(7years after terminating business relationship with the customer)
Client	Name, job title, work email address, work phone number, company you work for, criminal history or records	Accountants and Lawyers	Legitimate Interests pursuant to contract with SMS	(7years after terminating business relationship with the customer)
Client	Name, Nationality, Identification document number, residential address,	KYC and Due Diligence	Legal and Regulatory Obligations in relation to Public	(7years after terminating business relationship with the customer)



	<b>criminal history or records and position in a company.</b>		<b>Interests or Matters that affect the public</b>	
--	---	--	--	--

**Where Personal Data is processed because it is necessary for the performance of a contract to which you are a party, we will be unable to provide our services without the required information.**

### Conditions for processing Sensitive Personal Data

We will only process this data where we meet one of the conditions required by law for doing so. We may also ask for your explicit consent to process some categories of Sensitive Personal Data, but this is extremely rare.

We process this data when we collect or process information about your physical or mental health, or disability status, to ensure your health and safety in the workplace, to assess your fitness to work, and to provide appropriate workplace adjustments.

### Retention Period

We will retain your Personal Data for as long as is necessary to provide the services which you have requested from us. Your information is securely stored on [where it is stored].

However, we may need to retain some records for a longer period where this is required for us to be able to comply with our legal obligations.

We may also need to retain your Personal Data for a longer period where this is required in relation to legal claims, although this is rare.

We retain your personal data in accordance with the retention periods set out in the table above.

We will then dispose your information by [how this will be deleted].

## **8. Marketing**

We, including our branch in Singapore, would like to send you information about our products and services, events and news, which may be of interest to you. You consent to us receiving our marketing materials via email, telephone or social media.

You have the right to withdraw your consent to your personal data being used for direct marketing purposes at any time. You can do this as follows:

- contacting us at [marketing@sovereigngroup.com](mailto:marketing@sovereigngroup.com)
- 
- using the 'unsubscribe' link in emails.

For more information on how we use your personal data for marketing purposes, please see Sovereign Group [Marketing Privacy Notice](#).

## **9. Sharing your Personal Data**

In the course of providing you with this product/service – we may need to share your Personal Data with the following third parties:

- Regulators/Authorities;
- Banks/ Financial Institutions;
- Insurers;
- Professional service providers such as legal advisors, tax consultants, accountants, and eligible introducers; and
- Other third parties if required for the purposes of the products/services.

## 10. International Transfers

Where necessary, your Personal Data may be shared within the Sovereign Group. This may include transferring your Personal Data to other Group offices.

We may also share your Personal Data with 3rd party service providers. If we do so, we will enter into appropriate contractual arrangements to oblige the entities in those countries to operate to appropriate data protection standards:

- In the EU/EEA these standards include Standard Contractual Clauses (SCCs) approved by the European Commission, which contractually oblige the entities in those countries to operate to the data protection standards expected within the EU/EEA.
- In APEC countries organisations that hold a 'specified certification' that is granted or recognised under the law of the country or territory to which Personal Data is transferred will be taken to be bound by such legally enforceable obligations. Under the Personal Data Protection Regulations, a 'specified certification' refers to certifications under the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR) System and the APEC Privacy Recognition for Processors (PRP) System.

In such cases, our service providers and suppliers are data processors and may only use the data in line with our instructions and not for any other purpose. This and other obligations are agreed in the data processing contract between us.

## 11. How we protect Personal Data

SMS takes the security of your data seriously. We have implemented appropriate technical and organisational measures to safeguard your Personal Data and protect it from accidental or unlawful destruction, loss, or alteration and from unauthorised disclosure or access.

Where we engage 3<sup>rd</sup> parties to process Personal Data on our behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of the data.

## 12. Data subject rights

As per the PDPA, you have certain rights in relation to the processing of your Personal Data, including (but not limited to):

- **Request Access** to your Personal Data (commonly known as a "Subject Access Request"). This enables you to receive a copy of the personal data we hold about you and to check we are lawfully processing it. There are certain exceptions whereby organisations are allowed to withhold access to an individual's Personal Data. The withholding of information can be appealed to the PDPC. There is a fee involved.
- **Request Rectification** of the Personal Data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected. There are certain exceptions to the information you may request to rectify whereby organisations are obliged to correct. No fees.
- **Request Erasure** of your Personal Data. The PDPA does not provide individuals with a standalone right to request for an organisation to destroy or delete the Personal Data

in the organisation's possession or control. However, under the Retention Limitation Obligation, organisations are required to cease to retain Personal Data if retention of such Personal Data is no longer necessary for legal or business purposes.

- **Right to Withdraw Consent to processing** of your Personal Data. Individuals have the right to withdraw their consent to the collection, use, or disclosure of their Personal Data at any time by giving reasonable notice. However, the withdrawal of consent will not affect any legal consequences arising from such withdrawal. In the event of your withdrawal of consent, the ability of SMS to effectively administer the rights and obligations arising from your engagement with SMS may be hindered or prevented.

#### How to exercise your rights

If you wish to exercise your rights, please email [dposingapore@sovereigngroup.com](mailto:dposingapore@sovereigngroup.com)

Where relevant, you will have to pay a fee to access your Personal Data (and you may need to pay to exercise your other rights).

We may need to request specific information from you to help us confirm your identity before we can process a request from you to exercise any of the above rights. This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Upon SMS's receipt of your request, we will endeavour to fulfil your request as soon as reasonably possible. In some cases, such as with complex requests, it may take longer than this and, if so, we will keep you updated.

### **13. How to complain**

You have the right to lodge a complaint with the PDPC, if you believe SMS is infringing the data protection laws or you are concerned about the way in which we are handling your Personal Data.

The supervisory authority in the Republic of Singapore is the PDPC. You can find further [contact details on their website at PDPC | Personal Data Protection Complaint](#).

The supervisory authority in the Republic of Singapore is the PDPC. You can either submit a complaint electronically via the PDPC's [e-form](#) or send a mail to the following address:

Personal Data Protection Commission  
10 Pasir Panjang Road #03-01 Mapletree Business City  
Singapore 117438

### **14. What if you do not provide Personal Data to us**

Certain information, such as contact details, immigration status and payment details, may be required to allow SMS to provide the services that you have engaged us for. If you do not provide the required information this will hinder or prevent us from performing our required job scope, pursuant to a contract or legitimate interest, as the case may be.



If you wish to contact us in relation to this privacy notice or if you wish to exercise any of your rights outlined above, please contact our Data Protection Officer as follows:

Name: Andrew Gordon Galway

Email Address: [dposingapore@sovereigngroup.com](mailto:dposingapore@sovereigngroup.com)

Telephone: +65 6222 3209

## **15. Changes to this privacy notice**

We may update this notice (and any supplemental privacy notice), from time to time. Any changes will become effective as on Effective Date, when we post the revised Notice on our website. You are strongly advised to review this Notice periodically for any changes .

Last modified [7<sup>th</sup> June 2024]