

CLIENT PERSONAL DATA PROTECTION POLICY

1 INTRODUCTION

- 1.1 Camelot Trust Pte Ltd (the “**Company**”) recognises the importance of safeguarding personal data when dealing with information relating to its clients, and is committed to fully implementing and complying with the provisions of the Personal Data Protection Act (the “**Act**”). The Company’s Data Protection Policy set out here explains the systems in place to comply with the Act (the “**Policy**”), in respect of personal data as defined under the Act. A client’s engagement or continued engagement of the Company’s services upon having been notified of this Policy shall be deemed as consent to the provisions of this Policy.
- 1.2 The reference “client” herein refers to a client of the Company. The reference to personal data of a client refers to the personal data of a client and/or its representatives.

2 DATA PROTECTION OFFICER

- 2.1 The Company has appointed a Data Protection Officer (the “**DPO**”) to deal with day-to-day data protection matters and complaints, and to encourage good data handling practices within the Company. If a client has any questions, complaints or concerns, the client may contact the DPO as follows:

Name of DPO: Susanne Shaw
Email address of DPO: susanne@camelottrust.com
Telephone number of DPO: +65 6325 0970

3 WHAT IS PERSONAL DATA?

- 3.1 Personal data is data about an individual who can be identified from that data; or from that data and other information to which the Company has or is likely to have access. Personal data does not include an individual’s business contact information, business title, or information about an individual which is publicly available. For the purposes of the provision of the Company’s services, personal data collected by the Company would generally include without limitation a client’s and/or client representative’s full name, address, telephone number, personal e-mail address, date and place of birth, nationality, race, religion, identity card or passport information, gender, marital status, financial and tax information and bank account numbers.
- 3.2 Where the client provides the Company with the personal data of any individual, the client warrants that, in doing so, he/it is validly acting on behalf of that individual in providing the personal data and has obtained the individual’s consent to the Company’s collection, use, and disclosure thereof in accordance with this Policy.

4 PURPOSES OF COLLECTION OF PERSONAL DATA

- 4.1 The Company receives or collects the personal data of its clients for reasonable purposes in carrying out its role as a corporate services company. The Company undertakes not to use any personal data collected for any purpose other than for which it was collected.

4.2 These purposes include:-

- (a) Communication;
- (b) Providing services to the client, examples of which are as follows:
 - i. Company Incorporation;
 - ii. Providing corporate secretarial services where we are not the company secretary;
 - iii. Acting as Company Secretary;
 - iv. Acting as individual directors and/or corporate directors;
 - v. Providing Nominee Shareholder;
 - vi. Acting as banking signatories;
 - vii. Assisting clients with opening of bank accounts and addressing the relevant bank's account opening procedural requirements;
 - viii. Business registration and establishment services (eg. obtaining licences from various regulatory authorities)
 - ix. Immigration services
 - x. Procurement of offshore companies for clients
 - xi. Setting up Limited Partnerships
 - xii. Acting as General Partner
- (c) Preventing crime, offences or any breaches involving, amongst other things, fraud and money laundering;
- (d) Conducting due diligence checks in order to comply with legal requirements or requirements of government authorities;
- (e) Complying with all legal, regulatory and tax requirements and the requirements of any government authorities;
- (f) Promotional and marketing purposes;
- (g) Disclosure to third parties for the reasons outlined at 8 below.

4.3 Should the Company require any personal data in its possession to be used for a purpose other than those for which consent was originally given, fresh consent will be sought in order to use the data for that new purpose.

5 DISCLOSURE TO THIRD PARTIES

5.1 To carry out the abovementioned purposes, the Company may disclose its clients' personal data to third parties within or outside Singapore. Such third parties include:

- (a) Governmental organisations or authorities to whom the Company is required by law to disclose the data, e.g. for tax purposes;
- (b) Individuals who are legally entitled to the data;
- (c) Companies related to the Company;
- (d) Third parties who provide the Company with data processing, administration, health, insurance or legal services, or other professional or management services; and
- (e) Anyone to whom the Company is otherwise required to disclose it, e.g. individuals seeking access to their own personal data.

5.2 Such disclosure to third parties outside Singapore shall only be to organisations who are required or agree to process the data with a comparable level of data protection as that required under Singapore law.

6 ACCESS AND CORRECTION

6.1 Subject to statutory exceptions, a client may make written requests to the DPO to access or correct some or all of their personal data in the Company's possession or under its control. A client may also make a written request to the DPO for information on the ways in which the client's personal data has been used or disclosed by the Company within a year before the client's request.

6.2 The Company endeavours to take all reasonable steps to ensure that personal data in its possession is accurate, up-to-date, and complete. If any personal data of the Company's client provided to the Company becomes inaccurate, such client should contact the Company's DPO to update and correct such personal data.

6.3 Unless the Company is satisfied on reasonable grounds that a correction should not be made, the Company shall correct the personal data. After the correction of the personal data, except as provided in 14 below, the Company shall send the corrected personal data to every other entity to which the personal data was disclosed by the Company within a year before the date the correction was made unless that other entity does not need the corrected personal data for any legal or business purpose.

6.4 If the Company's client consents, the Company may send the corrected personal data only to specific entities to which the personal data was disclosed by the organisation within a year before the correction was made.

6.5 The Company may charge a reasonable fee for the provision of access to personal data. The Company will endeavour to respond to a client's request for access or correction of its personal data within 30 days of the request.

7 RETENTION

7.1 The Company will retain personal data for as long as it is necessary to serve the purpose for which it has been collected. Once the data in the Company's possession is no longer necessary to serve the purpose for which it was collected or to comply with any legal requirements, the data will be destroyed or anonymised in a secure manner.

7.2 Given that the limitation period for actions in contract and tort is 6 years, the Company will retain records in relation to its contract with a client for 7 years from the date of termination of the contract.

8 PROTECTION

8.1 The Company endeavours to maintain all personal data in its possession securely. To this effect, the Company has put in place processes to ensure protection of data in its possession against unauthorised access, collection, use, disclosure, copying, modification, disposal or other risks. These include without limitation as follows:

- (a) all the Company's employees and service providers who are authorised to access clients' personal data are bound by confidentiality obligations in their respective agreements with the Company;
- (b) policies are in place to prevent breaches of the Personal Data Protection Act;
- (c) all personal data in the Company's possession is stored in locked cabinets or in password-protected electronic storage systems.

9 WITHDRAWAL OF CONSENT

9.1 A client may withdraw consent for the collection, use or disclosure of the client's personal data by the Company at any time, with reasonable notice. The Company should inform the client of the likely consequences of such withdrawal of consent, and cease collecting, using or disclosing the personal data.

9.2 A client's withdrawal of consent might result in the Company being unable to continue providing services to the client, the termination of any contractual relationship between the Company and the client, and/or a breach of certain obligations arising from the contractual relationship. In such event, the Company's legal rights and remedies are reserved.

10 COMPLAINTS

10.1 If a client is of the view that his data has been erroneously or improperly handled by the Company, the client may lodge a complaint by email with the DPO. Once a complaint has been received, the DPO will acknowledge receipt of the same, and will investigate/consider the complaint.

10.2 The outcome of the DPO's investigation/consideration will be communicated to the complainant in writing, notifying him of the outcome.

11 UPDATING THIS POLICY

11.1 This Policy may be updated from time to time to take account of changes in the Company's activities/services and/or to ensure compliance with any prevailing legal requirements. A client's continued engagement of the Company's services following notification of any updates shall constitute consent to the updated Policy. A client who wishes to obtain a copy of this Policy may do so by contacting the DPO as set out at paragraph 3 of this Policy.