ADANSONIA
FUND MANAGER PRIVATE LIMITED
WORKING TOGETHER

63 Chulia Street
#15-01
Singapore
049514
www.adansoniafundmanager.com.sg

DATA PROTECTION POLICY

Effective date: 18th July 2022

Last updated on 18th July 2022

1. INTRODUCTION

1.1 This data protection policy (the "**Policy**") applies to all data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which Adansonia Management Services (Singapore) Private Limited (the "**Company**") has or is likely to have access ("**Personal Data**").

1.2 This Policy sets out the basis which the Company may collect, use, disclose or otherwise process your Personal Data in accordance with the Personal Data Protection Act 2012 (No. 26 of 2012) of Singapore (the "**Act**"). This Policy applies to all Personal Data which the Company collects, uses and discloses regardless of the media on which such Personal Data is stored and all Personal Data in the Company's possession or under its control, including Personal Data in the possession of organisations which the Company has engaged to collect, use, disclose or process Personal Data for its purposes. (last portion is from Sample Clauses and Templates for Customers (published 17 October 2017), PDPC)

1.3 This Policy has been implemented following consultation with the board of directors of the Company. This Policy will be updated as necessary to reflect best practice in data protection, security and control and to ensure compliance with any changes or amendments made to the Act.

2. SCOPE

2.1 The Company recognises that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that the Company takes seriously at all times.

2.2 The Data Protection Officer of the Company ("**DPO**") is responsible for overseeing the implementation of this Policy and the Company's compliance with the Act.

3. PERSONAL DATA PROTECTION PRINCIPLES

3.1 The Company adheres to the obligations relating to the collection, use and disclosure of Personal Data as set out in the Act, which requires:

3.1.1 the Company to obtain consent from an individual before Personal Data of the individual is collected, used or disclosed for a particular purpose by the Company ("**Consent Obligation**");

3.1.2 the Company to notify the individual of the purpose(s) for which the Company intends to collect, use or disclose the individual's Personal Data on or before such collection, use or disclosure of the Personal Data ("**Notification Obligation**");

Business Registration Number: 202120022R

3.1.3 the Company to collect, use or disclose Personal Data only for purposes that a reasonable person would consider appropriate in the circumstances and, if applicable, have been notified to the individual concerned by the Company ("**Purpose Limitation**");

3.1.4 the Company to make a reasonable effort to ensure that the Personal Data collected by or on behalf of the Company is accurate and complete if the Personal Data is likely to be used by the Company to make a decision that affects the individual to whom the Personal Data relates or is likely to be disclosed by the Company to another organisation ("**Accuracy Obligation**");

3.1.5 the Company to cease to retain documents containing Personal Data, or remove the means by which the Personal Data can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which the Personal Data was collected is no longer being served by retention of the Personal Data, and retention is no longer necessary for legal or business purposes ("**Retention Limitation**");

3.1.6 the Company to protect Personal Data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risk ("**Protection Obligation**");

3.1.7 the Company not to transfer any Personal Data to a country or territory outside Singapore except in accordance with the requirements prescribed under the Act ("**Transfer Limitation**");

3.1.8 the Company to provide an individual, upon request, with his Personal Data in the possession or under the control of the Company and information about the ways in which the Personal Data has been or may have been used or disclosed by the Company within a year before the date of the request ("**Access Obligation**");

3.1.9 the Company to correct an error or omission in an individual's Personal Data that is in the possession or under the control of the Company upon request ("**Correction Obligation**"); and

3.1.10 the Company to develop and implement the necessary policies and procedures for the Company to meet its obligations under the Act and to make information about the Company's policies and procedures available on request ("**Accountability Obligation**"),

(collectively, the "**Data Protection Obligations**").

4. COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

4.1 In order for the Company to provide its services to you, it may be necessary for it to collect, use and disclose your Personal Data to a third party.

4.2 While the specific types of Personal Data you submit to the Company may vary depending on the relevant services provided to you by the Company and whether you maintain an account with the Company, some examples of Personal Data which the Company may collect from you include: (Sample Clauses and Templates for Customers (published 17 October 2017);

(a) your name and identification information (e.g. NRIC / passport number);

(b) your contact information such as your address, email address or telephone number;

(c) your nationality;

(d) your gender;

(e) your date of birth;

(f) your marital status;

(g) photographs and other audio-visual information;

(h) employment information; and

(i) financial information such as credit card numbers, debit card numbers or bank account information.

5. NOTIFICATION OF THE PURPOSES FOR THE COLLECTION, USE OR DISCLOSURE OF YOUR PERSONAL DATA

5.1 The Company shall ensure that you are informed in writing of the purposes for the collection, use or disclosure of your Personal Data, on or before collecting such Personal Data. (s 14(1)(a), s 20(1)(a) PDPA, Advisory Guidelines Key Concepts) This may occur when you are entering into a contract with the Company under which the Company requires certain Personal Data from you. (Advisory Guidelines Key Concepts) The Company's collection, use and disclosure of Personal Data are limited to the purposes for which you have been notified. (Advisory Guidelines Key Concepts)

5.2 The purposes for collecting, using and disclosing your Personal Data will be stated at an appropriate level of detail for you to determine the reasons and manner in which the Company will be collecting, using or disclosing your Personal Data. However, this does not mean that every activity that the Company will undertake in relation to the collection, use or disclosure of your Personal Data will be specified. (Advisory Guidelines Key Concepts)

5.3 Your Personal Data will generally be collected, used and disclosed by the Company for the following purposes:

	Categories of Personal Data	**Description of purpose(s)**
Collection of Personal Data	(a) your name and identification information (e.g. NRIC / passport number) (b) your contact information such as your address, email address or telephone number (c) your nationality (d) your gender (e) your date of birth (f) your marital status (g) photographs and other audio-visual information (h) Your tax residence	1. For the purposes of and in connection with processing your request to the Company to provide such services as you may specify 2. Responding to your queries and requests 3. Verifying your identity 4. Carrying out due diligence checks 5. Compliance by the Company and

		its agents with all applicable laws, regulations, rules, circulars, guidelines and notices 6. Assisting in law enforcement and investigations by the relevant authorities 7. Crime prevention 8. Providing such services as you may specify and agreed to by the Company and for related purposes such as updating and enhancing the Company's client records, carrying out analysis for management purposes and statutory returns 9. Lodging such information as may be required by the authorities 10. Protecting and enforcing the Company's contractual and legal rights and obligations 11. Such other purposes as may be notified to you by the Company (each a "**Purpose**" and collectively, the "**Purposes**")
	Financial information such as credit card numbers, debit card numbers or bank account information	For the Company's billing and payment purposes

Use of Personal Data	(a) your name and identification information (e.g. NRIC / passport number) (b) your contact information such as your address, email address or telephone number (c) your nationality (d) your gender (e) your date of birth (f) your marital status (g) photographs and other audio-visual information (h) your tax residence	For any or all of the Purposes
	Financial information such as credit card numbers, debit card numbers or bank account information	For the Company's billing and payment purposes
Disclosure of Personal Data	(a) your name and identification information (e.g. NRIC / passport number) (b) your contact information such as your address, email address or telephone number (c) your nationality (d) your gender (e) your date of birth (f) your marital status (g) photographs and other audio-visual information (h) Your tax residence	1. Such Personal Data will be transferred by the Company to another party outside Singapore as the Company's operations server is located in and administered from Mauritius. 2. Such Personal Data will be disclosed to the Company's service providers or professional advisers for the purposes of providing services as you may specify 3. Such Personal Data will be disclosed to government or regulatory authorities or law enforcement

		agencies if the Company is required by the applicable law to do so 4. Such Personal Data will be disclosed to any other party to whom you authorise the Company to disclose your Personal Data, or to any other party in connection with any Purpose

5.4 The Company will inform you in writing of any purpose for the use or disclosure of your Personal Data which you have not been previously so informed, before such Personal Data is used or disclosed for such purpose. (s 14(1)(a), s 20(1)(b) PDPA, Advisory Guidelines Key Concepts) In determining if Personal Data can be used or disclosed for a particular purpose without obtaining your fresh consent, the Company will consider whether: (Advisory Guidelines Key Concepts)

(a) the purpose is within the scope of the purposes for which you have originally been informed, e.g. if it would fall within the Company's servicing of its existing business relationship with you;

(b) consent can be deemed to have been given by you in respect of use or disclosure for that purpose; and

(c) the purpose falls within the exceptions from consent in the Third and Fourth Schedules to the Act.

5.5 Upon your request, the Company will inform you of the business contact information (e.g. email, telephone number) of the DPO, being a person who is able to answer on behalf of the Company any questions you may have about the collection, use or disclosure of your Personal Data. (s 14(1)(a), s 20(1)(c) PDPA)

5.6 If the Company collects your Personal Data from another organisation without your consent, on or before collecting the Personal Data, the Company must provide the other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with the Act. (s 20(2) PDPA)

5.7 The purposes stated pursuant to clauses 5.3, 5.4 and 5.6 above may continue to apply even in situations where your relationship with the Company (for example, pursuant to a contract) has been terminated or altered in any way, for a reasonable period thereafter (including, where applicable, a period to enable the Company to enforce its rights under any contract with you). (Sample Clauses and Templates for Customers (published 17 October 2017), PDPC)

6. HOW THE COMPANY COLLECTS YOUR PERSONAL DATA

6.1 The Company will obtain your **consent** to the collection, use or disclosure of your Personal Data for specified purpose(s) in writing. (Advisory Guidelines on Key Concepts) If your oral consent is obtained by the Company, the Company will document your oral consent in writing (e.g. by noting down in writing the fact that oral consent was provided by you for certain purposes, together with the

date and time of such consent) and will confirm the oral consent in writing with you (which may be in electronic form or other form of documentary evidence). (Advisory Guidelines on Key Concepts)

6.2 The Company will collect your Personal Data where it is provided to the Company voluntarily by you directly after you have been notified of the purposes for which the Personal Data is collected and you have provided written consent to the collection, use or disclosure of your Personal Data for those purposes. (Sample Clauses and Templates for Customers (published 17 October 2017), PDPC)

6.3 The Company may also collect your Personal Data from a third party source. In such situations, the Company will: (Advisory Guidelines Key Concepts)

(a) notify the third party source of the purpose(s) for which the Company is collecting, using and/or disclosing your Personal Data; and (Advisory Guidelines Key Concepts)

(b) carry out the appropriate due diligence to verify that the third party source can validly give consent for the collection, use and disclosure of your Personal Data on your behalf or that the third party source had obtained consent for disclosure of your Personal Data to the Company.

6.4 In exercising appropriate due diligence to verify that a third party source can validly give consent or has obtained consent from you, one or more of the following measures appropriate to the circumstances at hand may be adopted by the Company: (Advisory Guidelines Key Concepts)

(a) seeking an undertaking from the third party source through a term of contract between the Company and the third party source that the disclosure to the Company for the Company's purposes is within the scope of the consent given by you to the third party source;

(b) obtaining confirmation in writing from the third party source;

(c) obtaining, and documenting in an appropriate form, verbal confirmation from the third party source; or

(d) obtaining a copy of the document(s) containing or evidencing the consent given by you to the third party source to disclose your Personal Data to the Company.

6.5 Consent may be given, or deemed to have been given, by any person validly acting on your behalf for the collection, use or disclosure of your Personal Data. (s 14(4) PDPA) In order to obtain consent from a person validly acting on your behalf, the Company will notify such person of the purposes for which your Personal Data will be collected, used and disclosed and such person must have given consent for those purposes on your behalf. (Advisory Guidelines Key Concepts)

6.6 If you give, or are deemed to have given, consent to the disclosure of your Personal Data by an organisation to the Company for a particular purpose, you are deemed to have consented to the collection, use or disclosure of your Personal Data for that particular purpose by the Company. (s 15(2) PDPA)

6.6.1 For example, if you have subscribed to a service offered by another entity within the Adansonia group of companies (the "**Adansonia Group**"), such Adansonia entity could have obtained your consent to the collection, use and disclosure of your Personal Data for the purposes of marketing and promoting the services of such Adansonia entity and the other companies within the Adansonia Group. (Advisory Guidelines Key Concepts)

7. SITUATIONS WHEN YOU ARE DEEMED TO HAVE GIVEN CONSENT

7.1 You are deemed to have consented to the collection, use or disclosure of your Personal Data by the Company for a particular purpose if: (s 15(1) PDPA)

(a) you, withOut actually giving consent, voluntarily provide your Personal Data to the Company for that purpose;

(b) it is reasonable that you would voluntarily provide your Personal Data; and

(c) you are aware of the purpose for which your Personal Data will be collected, used or disclosed. (Advisory Guidelines Key Concepts)

7.2 You may be regarded as voluntarily providing your Personal Data if you take some action that allows the Personal Data to be collected by the Company, without actually providing the Personal Data yourself. In such a situation, the Company will ensure that there is evidence that you wanted to provide your Personal Data and took the action required for it to be collected by the Company. (Advisory Guidelines Key Concepts)

7.3 It must also be reasonable in the circumstances for you to have voluntarily provided your Personal Data for a particular purpose. (Advisory Guidelines Key Concepts)

7.4 The Company will review its business processes from time to time to determine the situations where actual consent should be obtained from its individual customers and clients instead of seeking to rely on the deemed consent of such individuals. (Advisory Guidelines Key Concepts) This Policy will be updated accordingly in line with any changes made in this respect.

8. SITUATIONS WHERE THE COMPANY NEED NOT OBTAIN YOUR CONSENT BEFORE COLLECTING, USING OR DISCLOSING YOUR PERSONAL DATA

8.1 The Company may collect, use or disclose your Personal Data without your consent or from a source other than yourself, only in the circumstances specified respectively in the Second Schedule, Third Schedule and Fourth Schedule to the Act.

8.2 An example of this would be when your Personal Data is publicly available, i.e. your Personal Data is generally available to the public. Your Personal Data is considered publicly available if it can be observed by reasonably expected means at a location or an event at which you appear and that is open to the public. (para 1(c) Second Schedule, para 1(c) Third Schedule, para 1(d) Fourth Schedule to the PDPA, s 2(1) PDPA)

8.3 Personal Data is generally available to the public if any member of the public can obtain or access such Personal Data with few or no restrictions. In some situations, the existence of restrictions may not prevent the Personal Data from being publicly available. (Advisory Guidelines Key Concepts)

8.4 As such, the Company considers Personal Data of individuals (e.g. directors and shareholders) obtained from the Accounting and Corporate Regulatory Authority of Singapore via a company search on a Singapore-incorporated company to be Personal Data which is publicly available.

9. DISCLOSURE OF PERSONAL DATA

9.1 The Company may disclose your Personal Data: (Sample Clauses and Templates for Customers (published 17 October 2017), PDPC)

(a) where such disclosure is required for performing obligations in the course of or in connection with the Company's provision of the goods or services requested by you; or

(b) to third party service providers, agents and other organisations which the Company has engaged to perform any of the Purposes listed in clause 5.3 above for the Company.

9.2 If your Personal Data collected by the Company is to be used or disclosed by another entity within the Adansonia Group for a particular purpose, the Company will obtain your consent to the disclosure of your Personal Data by the Company to the other entity in the Adansonia Group for that particular purpose. If such consent is obtained, you are deemed to have consented to the collection, use or disclosure of such Personal Data for that particular purpose by the other entity in the Adansonia Group. (s 15(2) PDPA)

9.3 Your Personal Data may be transferred from Singapore to Mauritius due to the storage of the Company's data on the Company's operations server located in Mauritius and the administration of such server from Mauritius. Please see clauses 14.1 to 14.2 below for more details.

10. WITHDRAWAL OF CONSENT

10.1 The consent that you provide for the collection, use and disclosure of your Personal Data will remain valid until such time it is being withdrawn by you in writing. You may withdraw your consent and request the Company to stop using and/or disclosing your Personal Data for any or all of the purposes listed above by submitting a notice to withdraw your consent in writing or via email to the DPO at the contact details provided above. (Sample Clauses and Templates for Customers (published 17 October 2017), PDPC)

10.2 Upon receipt of your written request to withdraw your consent, the Company will verify your identity and inform you of the likely consequences of withdrawing your consent, even if these consequences are set out somewhere else, e.g. in the service contract between you and the Company. (s 16(2) PDPA, Advisory Guidelines Key Concepts)

10.3 The likely consequences of you withdrawing your consent are as follows:

(a) The Company will cease to collect, use or disclose your Personal Data for the purpose specified by you. In other cases, the Company may not be able to continue providing services to you or there may be legal consequences involved. (Advisory Guidelines Key Concepts)

(b) Subject to the Retention Limitation, the Company must cease (and cause other organisations which process Personal Data on the Company's behalf (excluding the employees of such other organisations) ("**data intermediaries**") and the Company's agents to cease) collecting, using or disclosing your Personal Data, as the case may be, unless such collection, use or disclosure without your consent is required or authorised under the Act or other written law. (s 16(4) PDPA)

(c) Apart from its data intermediaries and agents, the Company is not required to inform other organisations to which it has disclosed your Personal Data of your withdrawal of consent. This does not affect the Company's obligation to provide, upon request, access to your Personal Data in its possession or control and information to you about the ways in which your Personal Data may have been disclosed. Hence, you may find out which other organisations your Personal Data may have been disclosed to and give notice(s) to withdraw your consent to those other organisations directly. (Advisory Guidelines Key Concepts)

10.4 In general, the Company seeks to give effect to your withdrawal notice within 10 business days from the day the Company receives your withdrawal notice. If the Company requires more time to give effect to your withdrawal notice, you will be informed of the time frame by which the withdrawal of consent will take effect. (Advisory Guidelines Key Concepts)

10.5 If you have withdrawn your earlier consent to the collection, use or disclosure of your Personal Data by the Company, but have subsequently provided fresh consent to the Company, the Company may collect, use or disclose your Personal Data within the scope of the fresh consent that subsequently provided by you. (Advisory Guidelines Key Concepts)

11. ACCURACY OBLIGATION

11.1 The Company is obliged under the Act to make a reasonable effort to ensure that the Personal Data collected by or on behalf of the Company is accurate and complete, if the Personal Data is likely to be used by the Company to make a decision that affects you or is likely to be disclosed by the Company to another organisation. (s 23 PDPA)

11.2 Personal Data must be accurate and, where necessary, kept up to date. Personal Data must be corrected or deleted without delay when inaccurate.

11.3 The Company will ensure that the Personal Data it uses and holds is accurate, complete, kept up to date and relevant to the purpose for which the Company collected it. The Company will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards and will take all reasonable steps to amend inaccurate or out-of-date Personal Data.

11.4 In order to ensure that Personal Data collected by the Company is accurate and complete, the Company will make a reasonable effort to ensure that: (Advisory Guidelines Key Concepts)

11.4.1 Personal Data collected directly from you or through another organisation is accurately recorded;

11.4.2 the Personal Data collected includes all relevant parts thereof (so that it is complete);

11.4.3 the appropriate reasonable steps have been taken to ensure the accuracy and correctness of the Personal Data; and

11.4.4 it has considered whether it is necessary to update the information.

11.5 The Company may presume that Personal Data provided directly by you is accurate in most circumstances. The Company may request you to provide a verbal or written declaration that the Personal Data provided by you is accurate and complete. In addition, where the currency of your Personal Data is important, the Company will take steps to verify that the Personal Data provided by you is up to date (for example, by requesting a more updated copy of the Personal Data before making a decision that will significantly impact you). (Advisory Guidelines Key Concepts)

11.6 If your Personal Data is collected from a third party other than yourself, the Company will obtain confirmation from the source of your Personal Data that the source had verified the accuracy and completeness of your Personal Data. The Company may also conduct further independent verification if it deems prudent to do so. (Advisory Guidelines Key Concepts)

11.7 Please update the Company if there are changes to your Personal Data by writing or sending an email to the DPO at the contact details provided above.

12. RETENTION LIMITATION

12.1 The Company must cease to retain documents containing your Personal Data, or remove the means by which the Personal Data can be associated with you, as soon as it is reasonable to assume that the purpose for which the Personal Data was collected is no longer being served by retention of the Personal Data, and retention is no longer necessary for legal or business purposes (s 25 PDPA).

12.2 Personal Data may be retained so long as one or more of the purposes for which it was collected remains valid. (Advisory Guidelines Key Concepts 18.4(a)(ii))

12.3 Legal or business purposes for which retention of Personal Data is necessary may include situations where: (Advisory Guidelines Key Concepts 18.4(b))

12.3.1 the Personal Data is required for an ongoing legal action involving the Company;

12.3.2 retention of the Personal Data is necessary in order to comply with the Company's obligations under other applicable laws, regulations, international, regional or bilateral standards which require the retention of Personal Data; or

12.3.3 the Personal Data is required for the Company to carry out its business operations, such as to generate annual reports, or performance forecasts.

12.4 Assuming there is no ongoing legal action involving the Company, your Personal Data would ordinarily be kept for at least 6 years from the conclusion of the business relationship between you and the Company.

12.5 Upon the expiry of 6 years from the conclusion of the business relationship between you and the Company, the DPO shall conduct an assessment of your Personal Data held by the Company and determine whether retention of such Personal Data is still necessary.

12.6 If a decision is made to cease to retain your Personal Data, the Company shall carry out any or all of the following: (Advisory Guidelines Key Concepts 18.9, 18.10)

12.6.1 return documents containing your Personal Data to you;

12.6.2 transfer documents containing your Personal Data to another person on your instructions;

12.6.3 destroy documents containing your Personal Data (e.g. by shredding them or disposing of them in an appropriate manner);

12.6.4 destroy or erase from the systems of the Company, its agents and data intermediaries all of your Personal Data that the Company no longer requires. This includes requiring third parties and agents and data intermediaries of the Company to delete such Personal Data where applicable;

12.6.5 remove the means by which your Personal Data may be associated with you (i.e. anonymise your Personal Data); or

12.6.6 ensure that the agents and data intermediaries of the Company no longer have access to documents containing your Personal Data and your Personal Data contained therein.

13. SECURITY, INTEGRITY AND CONFIDENTIALITY (PROTECTION OBLIGATION)

13.1 Personal Data in the Company's possession or under its control must be protected by reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. (s 24 PDPA)

13.2 The Company will develop, implement and maintain safeguards appropriate to the Company's size, scope and business, the Company's available resources, the amount of Personal Data that the Company owns or maintains on behalf of others and identified risks (including use of encryption and anonymisation techniques where applicable). The Company will regularly evaluate and test the effectiveness of these safeguards to ensure security of the Personal Data held by the Company.

13.3 The Company strives to ensure that all of its data intermediaries or cloud service providers it engages meet standards or have certifications equivalent to ISO27001 and the Tier 3 Multi-Tiered Cloud Security (MTCS) Certification Scheme or such other standard or certification as may be prescribed by the Personal Data Protection Commission of Singapore ("**PDPC**").

13.4 The Company has employed the following security arrangements to protect the Personal Data which it collects:

13.4.1 Users are authenticated at two levels before getting access to the server; connect through SSL VPN running on Sophos Firewall to get access to network and secondly authenticate through Active Directory Domain Services to get access to server resources.

13.4.2 When an authorized user opens an encrypted file, EFS decrypts the file in the background and provides an unencrypted copy to the application. Authorized users can view or modify the file, and EFS saves changes transparently as encrypted data. If unauthorized users try to do the same, they receive an "Access denied" error.

13.4.3 BitLocker complements EFS by providing an additional layer of protection for data stored on Windows devices. BitLocker protects the whole volume from offline attacks.

13.4.4 Servers are protected by Sophos Intercept X for Server which delivers protection that is top-rated by industry experts, combining server-specific features to create a comprehensive, defense-in-depth solution. Intercept X protects the server against anti-ransomware, block server exploits, deny hackers and lock down server feature which control exactly what can and can't run on your servers and get notifications for any unauthorized change attempts.

13.4.5 The company has also deployed Forcepoint Data Loss Prevention (DLP) on its server. Forcepoint DLP controls all the data with one Single Policy. Replace broad, sweeping rules with individualized, adaptive data security. Protect PII and PHI, company financials, trade secrets, credit card data and other pieces of sensitive customer data-even in images. Follow intellectual property (IP) in both structured and unstructured forms and stop low & slow data theft even when user devices are off network. With its predefined policy library, it ensures regulatory compliance across 80+ countries for GDPR, CCPA and more.

13.5 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, the Company strives to protect the security of your Personal Data and is constantly reviewing and enhancing its information security measures. (Sample Clauses and Templates for Customers (published 17 October 2017), PDPC)

14. TRANSFER LIMITATION

14.1 Please note that the Company's operations server and some selected outsourced functions are domiciled and administered from Mauritius. As a result, your Personal Data will likely be transferred out of Singapore to a server and outsourced service provider based in Mauritius and administered by Perrieri IT Solutions Limited and Adansonia Management Services Limited and/or such other service provider located outside Singapore.

14.2 Enhanced security features deployed on the server administered by Perrieri IT Solutions Limited include:

14.2.1 Users are authenticated at two levels before getting access to the server; connect through SSL VPN running on Sophos Firewall to get access to network and secondly authenticate through Active Directory Domain Services to get access to server resources.

14.2.2 EFS file encryption. BitLocker complements EFS by providing an additional layer of protection for data stored on Windows devices. BitLocker protects the whole volume from offline attacks.

14.2.3 Servers are protected by Sophos Intercept X for Server which delivers protection, combining server-specific features to create a comprehensive, defense-in-depth solution. Intercept X protects the server against anti-ransomware, block server exploits, deny hackers and lock

down server feature which control exactly what can and can't run on your servers and get notifications for any unauthorized change attempts.

14.2.4 The servers have also deployed Forcepoint Data Loss Prevention (DLP). Forcepoint DLP controls all the data with one Single Policy. Replace broad, sweeping rules with individualized, adaptive data security. Protect PII and PHI, company financials, trade secrets, credit card data and other pieces of sensitive customer data-even in images. Follow intellectual property (IP) in both structured and unstructured forms and stop low & slow data theft even when user devices are off network. With its predefined policy library, it ensures regulatory compliance across 80+ countries for GDPR, CCPA and more.

14.3 By signing and acknowledging this Policy below, you have indicated your acknowledgement that the Company's operations server and some selected outsourced functions are domiciled and administered from Mauritius and you give your consent for your Personal Data collected by the Company to be disclosed and transferred from Singapore to Perrieri IT Services Limited and Adansonia Management Services Limited and/or such other service provider for the purpose of storing and processing such Personal Data.

14.4 The Company has an obligation not to transfer Personal Data to a country or territory outside Singapore except in accordance with the requirements prescribed under the Act. (s 26 PDPA)

14.5 Before transferring your Personal Data overseas, the Company will take appropriate steps to: (reg 9(1) PDPR)

14.5.1 ensure that the Company will comply with its obligations under the Act in respect of the transferred Personal Data while it remains in the possession or under the control of the Company; and

14.5.2 check whether, and ensure that, the recipient of the Personal Data in the country outside Singapore is bound by legally enforceable obligations to provide the transferred Personal Data a standard of protection that is at least comparable to the protection under the Act.

14.6 The Company is taken to have satisfied its obligation under clause 14.5.2 above if you consent to the transfer of your Personal Data to the recipient in the country or territory outside Singapore. In order for you to have so consented: (reg 9(3)(a), 9(4) PDPR)

14.6.1 before your consent is given, you have been provided with a reasonable summary in writing of the extent to which your Personal Data to be transferred to that country or territory will be protected to a standard comparable to the protection under the Act;

14.6.2 the Company must not have required you to consent to the transfer as a condition of providing a product or service, unless the transfer is reasonably necessary to provide the product or service to you; and

14.6.3 the Company must not have obtained or attempted to obtain your consent for the transfer by providing false or misleading information about the transfer, or by using other deceptive or misleading practices.

14.7 The Company would also be taken to have satisfied its obligation under clause 14.5.2 above if: (reg 9(3) PDPR)

14.7.1 the transfer of the Personal Data to the recipient is necessary for the performance of a contract between you and the Company, or to do anything at your request with a view to you entering into a contract with the Company;

14.7.2 the transfer of the Personal Data to the recipient is necessary for the conclusion or performance of a contract between the Company and a third party which is entered into at your request;

14.7.3 the transfer of the Personal Data to the recipient is necessary for the conclusion or performance of a contract between the Company and a third party if a reasonable person would consider the contract to be in your interest; or

14.7.4 the Personal Data is publicly available in Singapore.

14.8 The recipient of an individual's Personal Data in a country or territory outside Singapore is taken to be bound by legally enforceable obligations to provide a standard of protection for the transferred Personal Data that is at least comparable to the protection under the Act if the recipient holds a specified certification that is granted or recognised under the law of that country or territory to which the Personal Data is transferred. (reg 10A(1) PDPR)

14.8.1 A specified certification in relation to a recipient of an individual's Personal Data refers to a certification under the Asia-Pacific Economic Cooperation Privacy Recognition for Processors System (where the recipient is a data intermediary) or (if the recipient is not a data intermediary) the Asia-Pacific Economic Cooperation Cross Border Privacy Rules System. (reg 10A(2) PDPR)

14.9 For the purposes of clause 14.5.2 above, legally enforceable obligations include obligations imposed on a recipient of Personal Data under any law or any contract requiring the recipient to provide a standard of protection for the Personal Data transferred to the recipient that is at least comparable to the protection under the Act and specifying the countries and territories to which the Personal Data may be transferred under the contract. (reg 10(1)(a), 10(1)(b), 10(2) PDPR)

14.10 If the Company transfers Personal Data to a recipient outside Singapore, the contract between the Company and such recipient should contain at least the following protections: (Advisory Guidelines Key Concepts)

If the recipient is a data intermediary	**If the recipient is an organisation which is not a data intermediary**
Contract should contain protections in relation to the: • Protection Obligation • Retention Limitation	Contract should contain protections in relation to the: • Purpose of collection, use and disclosure of Personal Data by the recipient • Accuracy Obligation • Protection Obligation • Retention Limitation • Policies on Personal Data protection • Access Obligation • Correction Obligation

1.1 Engaging cloud service providers

14.11 If the Company engages a cloud service provider, it is still responsible for complying with all obligations under the Act in respect of Personal Data processed by the cloud service provider on its behalf and for its purposes. (Advisory Guidelines on the PDPA for Selected Topics [8.1]) Processing is defined in the Act as the carrying out of any operation or set of operations in relation to the Personal Data, and includes recording, holding, organising, adapting or altering, retrieval, combination, transmission, erasure or destruction of Personal Data. (s 2(1) PDPA)

14.12 The cloud service provider engaged by the Company will be subject to the Protection and Retention Limitation Obligations under the Act and the cloud service provider's obligations in these areas will extend to Personal Data that it processes or hosts for the Company in data centres outside Singapore. (Advisory Guidelines on the PDPA for Selected Topics)

14.13 The Company will be responsible for complying with the Transfer Limitation in respect of any overseas transfer of Personal Data in using the cloud service provider's cloud services. This is regardless of whether the cloud service provider is located in Singapore or overseas. (Advisory Guidelines on the PDPA for Selected Topics)

14.14 If the Company engages a cloud service provider, the contract between the Company and the cloud service provider should: (Advisory Guidelines on the PDPA for Selected Topics)

14.14.1 contain an obligation on the cloud service provider to transfer Personal Data only to locations with comparable data protection regimes, or that the recipients (e.g. data centres or sub-processors) in these locations are bound by legally enforceable obligations to ensure a comparable standard of protection for the transferred Personal Data;

14.14.2 address the standard of protection for the Personal Data transferred overseas;

14.14.3 clearly state the overseas locations to which the Personal Data is transferred; and

14.14.4 contain assurances by the cloud service provider that all the data centres or sub-processors in overseas locations that the Personal Data is transferred to comply with standards equivalent to industry standards such as ISO27001 and Tier 3 of the Multi-Tiered Cloud Security (MTCS) Certification Scheme.

15. REQUEST TO ACCESS PERSONAL DATA (ACCESS OBLIGATION)

15.1 If you wish to make an access request for:

(a) access to your Personal Data that is in the Company's possession or under the Company's control; or

(b) information about the ways in which such Personal Data has been or may have been used or disclosed by the Company within a year before the date of your access request, (s 21(1) PDPA)

you should submit your request in writing or via email to the DPO at the contact details provided above.

15.2 Please state in your access request the reason(s) for making the access request, the type of Personal Data you require, the type of use and disclosure of your Personal Data you require and the time and date such Personal Data was collected from you. (reg 3(b) PDPR, Advisory Guidelines Key Concepts)

15.3 Upon receipt of your access request, the Company will exercise due diligence and adopt appropriate measures to verify your identity. (Advisory Guidelines Key Concepts [15.12]) Where a third party is making an access request on your behalf, the Company will ensure that the third party has the legal authority to validly act on your behalf. (Advisory Guidelines Key Concepts)

15.4 If the Company has transferred Personal Data to a data intermediary that is processing the Personal Data under the control of the Company, the Company's response to your access request must take into account the Personal Data which is in the possession of the data intermediary. (Advisory Guidelines Key Concepts)

15.5 The Company seeks to respond to your access request within 30 days after the access request is received by the Company. If the Company is unable to respond to an access request within this time period, you will be informed in writing within this 30-day period of the time by which the Company will be able to respond to the request and the Company shall endeavour to respond to your request as soon as reasonably possible. (reg 5 PDPR, Advisory Guidelines Key Concepts)

15.6 Please note that a reasonable fee may be charged for an access request. If so, the Company will inform you of a written estimate of such fee before processing your request. The Company need not respond to your access request unless you have agreed to pay the fee for services provided to you to enable the Company to respond to the access request. (Advisory Guidelines Key Concepts)

15.7 Please note that the Company is not obliged to provide access to the following types of information or documents:

15.7.1 Documents (or systems) which do not comprise or contain the Personal Data in question, as long as you are provided with the Personal Data that you have requested and are entitled to have access to under the Act. In the case of a document containing the Personal Data in question, only the Personal Data (or the sections of the document containing the Personal Data) may be provided to you if it is feasible to do so. (Advisory Guidelines Key Concepts)

15.7.2 Information which is no longer within the Company's possession or under its control when the access request is received. In such a situation, the Company will inform you that it no longer possesses the Personal Data and is thus unable to meet your access request. (Advisory Guidelines Key Concepts)

15.7.3 Information on the source of the Personal Data. (Advisory Guidelines Key Concepts)

15.7.4 Information or Personal Data which falls under the Fifth Schedule to the Act, which lists out various exemptions from the requirement to provide access to Personal Data. The Company is not prohibited from providing information in respect of the matters specified in the Fifth Schedule to the Act and may do so if it decides to. (Advisory Guidelines Key Concepts)

15.7.5 The Company is not required to provide you access to your Personal Data if the burden or expense of providing access would be unreasonable to the Company or disproportionate to your interest or if your request is otherwise frivolous or vexatious. (Advisory Guidelines Key Concepts)

15.8 The Company will not provide access to Personal Data in the following situations:

15.8.1 No individual or organisation should be informed that the Company has disclosed Personal Data to a prescribed law enforcement agency if the disclosure is necessary for any investigation or proceedings and the Personal Data is disclosed to an authorised officer of the agency. In this regard, the Company may refuse to confirm or deny the existence of Personal Data, or the use of Personal Data without consent for any investigation or proceedings, if the investigation or proceedings and related appeals have not been completed. (s 21(4) PDPA, reg 6 PDPR, Advisory Guidelines Key Concepts)

15.8.2 An access request shall not be acceded to if any of the grounds in section 21(3) of the Act are applicable, for example, where the provision of the Personal Data requested by you could reasonably be expected to reveal Personal Data about another individual.

However, where the provision of the Personal Data requested by you will reveal Personal Data about another individual, the Company would have to provide the access requested if the other individual has given consent to the disclosure of his Personal Data or any of the exceptions listed under the Fourth Schedule to the Act apply to the extent that the Company may disclose the Personal Data of the other individual without consent. (Advisory Guidelines Key Concepts)

15.9 Access to the Personal Data you requested for may be provided in the following forms (reg 4(2) PDPR):

15.9.1 A copy of your Personal Data and use and disclosure information may be provided to you in documentary form upon your request. The Company has the option of charging a reasonable fee for producing the copy. (Advisory Guidelines Key Concepts)

15.9.2 If the requested Personal Data resides in a form that cannot practicably be provided to you in documentary form, whether as physical or electronic copies (for example, the data cannot be extracted from a special machine owned by the Company), then the Company may provide you a reasonable opportunity to examine the requested Personal Data and use and disclosure information in person. (Advisory Guidelines Key Concepts)

15.9.3 If the Personal Data requested can be retrieved by yourself (e.g. resides in online portals in which access has been granted by the Company), the Company will inform you how you may retrieve the Personal Data requested. (Advisory Guidelines Key Concepts)

15.10 The Company will respond to your access request by providing access to the Personal Data requested or by informing you of a rejection of the access request where the Company has valid grounds not to provide access. (Advisory Guidelines Key Concepts)

15.11 If your access request is rejected:

15.11.1 the Company will provide you a reply informing you of the relevant reason(s) why the access request was rejected; and (Advisory Guidelines Key Concepts)

15.11.2 the Company will preserve a copy of the withheld Personal Data for a period of at least 30 calendar days after your access request is rejected in case a review of the Company's decision is sought. (Advisory Guidelines Key Concepts)

16. REQUEST TO CORRECT PERSONAL DATA (CORRECTION OBLIGATION)

16.1 The Company must correct an error or omission in the Personal Data about an individual that is in its possession or under its control as soon as practicable when the individual requests for such a correction, unless the Company is satisfied on reasonable grounds that a correction should not be made. (s 22(1), s 22(2)(a) PDPA)

16.2 If you wish to make a correction request to correct or update any of your Personal Data which the Company holds about you, you may submit your request in writing or via email to the DPO at the contact details provided above.

16.3 Please note that no fees are payable for the correction of your Personal Data. (Advisory Guidelines Key Concepts)

16.4 If the Company has transferred Personal Data to a data intermediary that is processing the Personal Data under the control of the Company, the Company's response to your correction request must take into account the Personal Data which is in the possession of the data intermediary. (Advisory Guidelines Key Concepts)

16.5 Upon receipt of your correction request, the Company will exercise due diligence and adopt appropriate measures to verify your identity.

16.6 The Company seeks to make the correction to your Personal Data within 30 days after receiving your correction request. If a decision is made not to correct your Personal Data, the Company seeks to, within 30 days after receiving your correction request, annotate on your Personal Data the requested correction that was not made and provide reasons why such correction was not made. If the Company is unable to respond to your correction request within 30 days after receiving the request, you will be informed in writing within this 30-day period of the time by which the Company will be able to correct your Personal Data. (s 22(5) PDPA, reg 5 PDPR, Advisory Guidelines Key Concepts)

16.7 In deciding whether a correction should be made to your Personal Data, please note that the Company is not required to correct or otherwise alter an opinion, including a professional or an expert opinion. (s 22(6) PDPA) The Company is also not required to make a correction in respect of the matters specified in the Sixth Schedule to the Act.

16.8 If a decision is made not to correct your Personal Data, an annotation should be made to your Personal Data in the Company's possession or under its control indicating the correction that was requested but not made. (s 22(5) PDPA)

16.9 If a decision is made to correct your Personal Data, the corrected Personal Data will be sent to every other organisation to which the Personal Data was disclosed by the Company within a year before the date the correction was made, unless that other organisation does not need the corrected Personal Data for any legal or business purpose. (s 22(2)(b) PDPA) However, the corrected Personal Data may be sent only to specific organisations to which the Personal Data was disclosed by the Company within a year before the date the correction was made, provided that you have consented to the same. (s 22(3) PDPA)

16.10 If the Company receives a notification from another organisation of a correction of your Personal Data which has been previously disclosed to the Company by that other organisation, the Company should decide within 30 days of the receipt of the notification from the other organisation whether to correct such Personal Data. In making its decision, the Company will have regard to the considerations in clause 16.7 above.

17. ACCOUNTABILITY OBLIGATION

17.1 The Company must implement the necessary policies and procedures in order to meet its obligations under the Act and shall make information about its policies and procedures available on request. (s 12 PDPA)

17.2 The Company is required to implement appropriate technical and organisational measures in an effective manner, to ensure compliance with the Data Protection Obligations. The Company is responsible for, and must be able to demonstrate, compliance with the Data Protection Obligations.

17.3 The Company must have adequate resources and controls in place to ensure and to document compliance with this Policy, including regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of such tests to demonstrate compliance.

18. CHANGES TO THIS POLICY

18.1 This Policy applies in conjunction with any other notices, contractual clauses and consent clauses that apply in relation to the collection, use and disclosure of your Personal Data by the Company. (Sample Clauses and Templates for Customers (published 17 October 2017), PDPC)

18.2 The Company may revise this Policy from time to time without any prior notice. You may determine if any such revision has taken place by referring to the date on which this Policy was last updated. Your continued use of the Company's services constitutes your acknowledgement and acceptance of such changes. (Sample Clauses and Templates for Customers (published 17 October 2017), PDPC)