

Segantii Capital Management Limited

Privacy Policy

Last updated: February 2023

This Privacy Policy sets forth the privacy practices of Segantii Capital Management Limited (“Segantii,” “we,” “our,” or “us”) and its affiliates with respect to our collection, use, sharing, and disclosure of personal data, including, but not limited to, personal data collected through this website, how it is used, and the circumstances under which it may be shared and disclosed. This Privacy Policy constitutes a legally binding agreement between you and Segantii that conditions your use of the website, where and as permitted by applicable law.

If you are a California resident, please also read our Privacy Notice for California Consumers below.

Personal information collection and privacy policy statements

When you visit the website or during our ordinary business activities, we may collect or ask you to provide certain nonpublic personal information (“personal data”) in order to help us manage our relationship with you and serve your investment needs. By using or accessing this website and providing us with your personal data, you accept and consent to the practices described in this Privacy Policy. The personal data which you have provided to us will at all times be governed by applicable law, including the terms of the Personal Data (Privacy) Ordinance, as amended and supplemented from time to time (the “Ordinance”).

Provision of your personal data is voluntary. However, failure to provide your personal data may result in us being unable to provide you with our services.

You may wish to visit the official website of the Office of the Privacy Commission <https://www.pcpd.org.hk> for more information about the Ordinance.

Your personal data

We value our clients and appreciate the trust you have placed in us. It is our policy to protect our clients' privacy and this policy also applies to the privacy of users of the website.

In order to provide you with our services, we may collect and maintain certain personal data about you. The personal data we may collect from you may include personally identifiable information including names, residential or business addresses, or other contact details, signature, nationality, tax identification or passport number, date of birth, place of birth, photographs, copies of identification documents, bank account details, information about assets or net worth, credit history, information on investment activities, or other personal information, such as certain special categories of personal data (including, where relevant, information on political affiliations, ethnic origin, or criminal convictions), as specified under applicable law, that may be contained in the relevant materials, documents, or obtained through background searches.

Purpose of collection and use of your personal data

We may collect personal data from: (i) your communications with us; (ii) your transactions with us; (iii) service providers; and (iv) affiliates. We use personal data for the following business purposes:

- To provide our products and services and serve your investment needs;
- To provide customer service and process your requests and inquiries;
- To offer new information, products and services;
- For account maintenance;
- To communicate with you;

- To protect the security and integrity of the website;
- To prevent or investigate fraud or other unlawful activity, and detect security incidents; and
- To comply with and enforce applicable legal or regulatory requirements.

Direct marketing

We may use your personal data in direct marketing of one or more of the following products / services: (i) collective investment schemes managed, advised, distributed or promoted by us, (ii) asset management, investment advisory, wealth management or any other investment related services, (iii) other investment opportunities, and (iv) any other financial or investment products or services.

We may not use your personal data for direct marketing purposes unless we have received your consent for such use.

You may, at any time and without charge, request that we cease using your personal data for direct marketing purposes by sending an email stating this to compliance@segantii.com.

Retention of your personal data

We will limit the amount of personal data we collect and limit the amount of time we store such information, to the amount reasonably necessary to accomplish our business purposes (including for the purpose of marketing our products and services), or to comply with applicable laws.

Disclosure

Your personal data will generally be kept confidential and will not be disclosed to any other person without your consent, except as described in this Privacy Policy. Access to your personal data is restricted to our employees who need access to that personal data to provide products or services to you.

However, in order for us to effect transactions that you request or authorise or to notify you of other financial products and services that we offer, we may disclose the personal data we collect, as described above, to companies that perform administrative and or marketing services on our behalf, such as administrators, transfer agents, custodians and distributors as well as those that provide professional, legal, or accounting advice to us. These service providers will use this information only for the services for which we engaged them, and are not permitted to use or share this personal data for any other purpose.

We may also disclose your personal data where we are required to do so by law or when responding to proceedings of a court of law or similar legal process, to protect against fraud, and to otherwise cooperate with law enforcement or regulatory authorities.

We do not sell your personal data to any third party or transfer your personal data to any third party for use by such third party in direct marketing. However, your personal data may be transferred to another company if there is a sale or merger of Segantii or the division responsible for these services.

Security

Segantii seeks to safeguard personal data. We have installed security systems to ensure your personal data are not subject to unauthorised access. We restrict access to our client's personal data to employees or other personnel requiring that personal data to provide our products or services.

Your right of access to and to correct personal data

You are entitled, in accordance with the Ordinance, to check whether we hold data about you, the kinds of data held by us and to have access to those data. If any of these data are incorrect or inaccurate, you have the right to correct or update them. Requests for access to or to correct personal data should be addressed to niral.maru@segantii.com. In accordance with the Ordinance, we are entitled to charge a reasonable fee for processing any data access requests.

You are also entitled to request that we describe our policies and practices in relation to personal data.

Changes to the Privacy Policy

We reserve the right to amend, add to, or remove any of the provisions in this Privacy Policy at any time. You should read this page regularly to ensure you are updated as to any changes. However, if any change involves a plan to use your personal data in a way that differs from this Privacy Policy, we will first send you an email to obtain your prior consent. However, your continued access to the website after such changes conclusively demonstrates your consent to any changes.

Enquiries

If you have questions or concerns about our Privacy Policy in relation to your personal data, please contact us by email at compliance@segantii.com or by mail at Segantii Capital Management Limited, 21st Floor, 100 QRC, 100 Queen's Road Central, Hong Kong.

Privacy Notice For California Consumers

Last updated: February 2023

This notice contains disclosures required by the California Privacy Rights Act ("CPRA"). Terms defined in the CPRA have the same meaning when used in this notice. This notice is only relevant to California residents ("consumers" or "you"). Consumers with disabilities may access this notice via this printable copy in pdf format.

Information We Collect. In the past 12 months, we have collected and shared for a business purpose the following categories of personal information ("Personal Information"):

Category	Examples
Identifiers	A real name, alias, email address, postal address, other contact details, Internet Protocol (IP) address, account name, copies of identification documents, Social Security number, driver's license number, tax identification or passport number, or other similar personal identifiers.
Other personal information categories, as listed in the California Customer Records Statute	A signature, telephone number, employment, bank account number, information about assets or net worth, credit history, information on investment activities or any other financial information.
Protected classification characteristics under California or U.S. federal law	Age (40 years or older), nationality, race, citizenship, marital status, sex, veteran or military status.

Commercial information	Account activity, records of products or services purchased, obtained, or considered, or other purchasing histories.
Internet or other similar network activity	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.
Sensory data	Audio recordings of telephone calls
Professional or employment-related information	Current or past job history
Inferences drawn from other personal information	Profile reflecting a person's preferences, characteristics and interests.
Sensitive personal information	A consumer's SS, driver's license, state ID card, or passport number; account log-in or debit/credit card number in combination with any access code, password, or account credentials; precise geolocation; racial/ethnic origin, religious/philosophical beliefs, or union membership; contents of mail, email, and text messages; genetic data; biometric information; PHI; or sex life or sexual orientation.

Personal Information does not include information that is publicly available, de-identified/ aggregated, or subject to HIPAA or GLBA.

We collect Personal Information from the following categories of sources:

- Your communications with us;
- Our agents and service providers
- Our affiliates;
- Information generated through use of our website; and
- Entities we do business with.

We also may receive your personal data from other third parties or sources, such as the administrator, publicly accessible databases or registers, tax authorities, governmental agencies and supervisory

authorities, credit agencies, fraud prevention and detection agencies, or publicly accessible sources, such as the Internet.

We do not knowingly collect, solicit or sell Personal Information from anyone under the age of 16 without the prior consent of a parent or guardian.

Purpose for Collection and Use of Personal Information. We may collect or use Personal Information for one or more of the following purposes:

- Providing you with information about our products and services;
- Providing you with performance and other updates;
- One or more of the following business purposes:
 - Performing services (for us or our service provider) such as account servicing, processing orders and payments, and analytics;
 - Auditing related to our interactions with you (e.g., auditing compliance);
 - Legal compliance;
 - Detecting and protecting against security incidents, fraud, and illegal activity;
 - Debugging;
 - Internal research for technological improvement;
 - Internal operations; and
 - Activities to maintain and improve our services.

Sharing Personal Information. We may disclose Personal Information in one or more of the categories identified above to:

- Agents and service providers, including, but not limited to: the administrator, transfer agent, custodian, distributors, brokers, auditors, legal advisors, law firms, financial advisors, and/or consultants;
- Affiliates;
- Business partners;
- Legal or government regulatory authorities and/or self-regulatory organizations as required by applicable law; and
- In connection with a potential business transfer.

In the past 12 months, we have not sold any Personal Information we collect to third parties, and we have shared the categories of personal information we collect only as set forth above.

Length of Time. We will keep your Personal Information for as long as necessary to comply with our regulatory obligations.

Rights of California Consumers. The CPRA provides a California consumer the following rights, subject to certain exceptions and limitations:

- The right to request: (a) the categories and specific pieces of Personal Information we collect about you; (b) the categories of sources from which we collect your Personal Information; (c) our purposes for collecting, selling or sharing your Personal Information; (d) the categories of Personal Information disclosed for a business purpose and the categories of persons to whom it was disclosed; (e) the categories of your Personal Information (if any) that we have either sold, shared, or disclosed.
- For certain categories of Personal Information, the right to request a list of what we disclosed to third parties for their own direct marketing purposes in the past 12 months and the names and addresses of those third parties.
- The right to request that we delete your Personal Information, subject to certain exceptions.
- The right to opt out of our sale(s) (if any) of your Personal Information.
- The right to request we correct any inaccurate Personal Information maintained about you.

- The right to limit our use of your sensitive personal information to only use that is necessary to perform the services expected or provide the goods reasonably expected.
- The right not to receive discriminatory treatment for exercising your CPRA rights.

You may submit requests relating to your exercise of CPRA rights to us via:

phone at +852 3926 8388;

or

email to Compliance@segantii.com.

All verifiable requests must provide (1) enough information that allows us to reasonably verify you are the person about whom we collected Personal Information or an authorized representative and (2) sufficient detail that allows us to properly evaluate and respond to it.

We endeavor to respond to a verifiable request within 45 days of its receipt. If we require more time, we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically, at your option.

You may designate an authorized agent to make a CPRA request on your behalf. In such case, we will ask the agent to provide proof that you have given the agent signed permission to act on your behalf. In addition, we will ask you to (1) verify your identity directly with us in the manner described above and (2) directly confirm with us that you have provided the agent permission to make the request on your behalf.

You may only make a verifiable request for access or data portability twice within a 12-month period.

Questions

If you have questions regarding this Notice, please contact us at Compliance@segantii.com.