Banque Heritage SA
61 route de Chêne, PO Box 6600
CH – 1211 Geneva 6, SWITZERLAND
Tel. +41 (0)58 220 00 00 Fax +41 (0)58 220 00 01
www.heritage.ch

BANQUE HERITAGE

DATA PROTECTION AND PRIVACY NOTICE

Protection of its clients' data is clearly of major importance to Banque Heritage Ltd and high protection standards have been set in place. This privacy notice contains general information on the type of personal data Banque Heritage SA collects, what it does with that information, and the rights given to its clients.

I. WHAT PERSONAL DATA IS COLLECTED BY BANK HERITAGE?

Bank Heritage Ltd (hereinafter referred to as the "Bank") will, depending on the product or service provide, collect and process personal data, i.e. any information that relates to an identified or identifiable natural person (hereinafter the "Data") which includes:

a. personal details such as name, identification number, date of birth, national identity card or passport, phone number(s), physical and electronic address, and family details such as the name of your spouse, partner, or children;
b. financial information and information relating to the assets (including real estate properties), financial statements, liabilities, revenues, earnings and investments (including investment objectives) of the client;
c. tax domicile and other tax-related documents and information;
d. where applicable, professional information such as work experience, knowledge of, and experience in, investment matters;
e. details of the products and services the client uses;
f. any records of phone calls with the Bank;
g. client or account number;
h. when the client accesses our Website, data transmitted by his/her browser and automatically recorded by our server, including date and time of the access, name of the accessed file as well as the transmitted data volume and the performance of the access, the web browser, browser language and requesting domain, and IP address;
i. to the extent legally possible, information relating to criminal convictions or offences. In some cases, the Bank collects this information from public registers or other third-party sources, such as wealth screening services, credit reference agencies, fraud prevention agencies;
j. if relevant, the Bank will also collect information about card holders or additional account holders, business partners (including other shareholders or beneficial owners), dependants or family members, representatives, and agents. Additionally, the Bank will also collect information about directors, employees or shareholders of institutions and companies.

II. LEGAL BASIS FOR PROCESSING DATA

Processing of Data is founded on Swiss legal and regulatory basis. In particular, the purposes of processing Data include the following:

- to enable the Bank to enter into or executing a contract for the services or products you requested by the client, or for carrying out the Bank's obligations under such a contract;
- to enable the Bank to meet its legal or regulatory responsibilities;
- to enable the Bank to make the required disclosures to authorities, regulators and government bodies;
- to enable the Bank to meet its accountability and regulatory requirements.

Where the Data the Bank collects from the client is needed to meet our legal or regulatory obligations or enter into an agreement with you, and if the Bank cannot collect this Data, there is a possibility we may be unable to on-board the client or provide products or services.

III. PURPOSES OF PROCESSING

We always process your Data for a specific purpose and only process the Data which is relevant to achieve that purpose. In particular, the Bank processes Data for the following purposes:

a. client on-boarding processes, including to verify identity and to conduct legal and other regulatory compliance checks (for example, to comply with anti-money laundering regulations and prevent fraud);
b. providing products and services and ensuring their proper execution, for instance by ensuring that the Bank can identify the client and make payments to and from the accounts in accordance with instructions received and the product terms;
c. managing the relationship with the client, including communicating with him/her in relation to the products and services, handling customer service-related queries and complaints, facilitating debt recovery activities, and closing the account (in accordance with applicable law) if it remains dormant and we are unable to contact the client after a period of time;
d. taking steps to improve our products and services and our use of technology, including testing and upgrading of systems and processes;
e. contacting the client for direct marketing purposes about products and services ;
f. meeting our on-going regulatory and compliance obligations (e.g. laws of the financial sector, anti-money-laundering and tax laws), including in relation to recording and monitoring communications, disclosures to tax authorities, financial service regulators and other regulatory and governmental bodies, and investigating or preventing crime;
g. ensuring the safety of our customers, employees and other stakeholders;
h. any other purposes the Bank may notify the client from time to time.

IV. ACCESS TO DATA

1. <u>Within Heritage's Group</u>

The Bank may share Data within the Bank's Group companies in order to ensure a consistently high service standard across our group and to provide services and products to you.

2. Access to Data by Third Parties

When providing products and services to you, the Bank may share Data with persons acting on behalf of the client or otherwise involved in the transaction (depending on the type of product or service received), including, where relevant, the following persons and parties:

a. companies in which you have an interest in securities where such securities are held by the bank for you;
b. payment recipients, beneficiaries, account nominees, intermediaries and correspondent banks;
c. clearing houses and clearing or settlement systems; and specialised payment companies or institutions such as SWIFT;
d. credit card issuers and other card payment and platform providers;
e. market counterparties;
f. swap or trade repositories;
g. stock exchanges;
h. other financial institutions, credit reference agencies or credit bureaus (for the purposes of obtaining or providing credit references);
i. any third-party fund manager who provides asset management services to the client and any introducing broker to whom we provide introductions or referrals;
j. any third party or their representatives seeking to protect its legal rights or such rights of others.

3. Service providers

In some instances, we also share Data with our suppliers and other business partners who provide services to us, such as IT and hosting providers, marketing providers, communication services and printing providers, debt collection, tracing, debt recovery, fraud prevention, credit reference agencies and others. The Bank takes steps to ensure they meet our data security standards, so that the Data remains secured.

4. Public or regulatory authorities

If required from time to time, the Bank shall disclose Data to public authorities, regulators or governmental bodies, including when required by law or regulation, under a code of practice or conduct, or when these authorities or bodies require the Bank to do so.

V. INTERNATIONAL TRANSFERS OF DATA

The recipients referred to above may be located outside Switzerland. In those cases, except where the relevant country has been determined by the Federal Data Protection Commissioner to provide an adequate level of protection, the Bank requires such recipients to comply with appropriate measures designed to protect Data within a binding legal agreement. The Bank implements the necessary legal, operational and technical measures in this respect.

VI. HOW LONG DOES THE BANK STORE DATA?

In general, the Bank will retain Data for the entire period of the business relationship plus 10 years, subject to any legal or regulatory requirement that may foresee a longer period of retention. Beyond that, the Bank will only retain personal data for as long as necessary to fulfil the purpose for which it was collected or to comply with legal, regulatory or internal policy requirements.

The Swiss Financial Market Supervisory Authority ("FINMA") requires that the Bank record external and internal telephone calls of employees engaged in securities trading and store electronic correspondence (emails, communication via Bloomberg or Reuters, etc.) and evidence of the calls made on business telephones by these employees for a period of two years to make this information available to FINMA on request. This obligation also applies to employees identified by a risk-based assessment as being highly exposed to information that might be relevant to market supervision. The Bank furthermore stores incoming and outgoing business and private communication data, in particular emails with attachments, chats and instant messaging, in a separate and protected archive located in Switzerland.

VII. CLIENTS' RIGHTS

The Bank's client has the following rights:

- right to ask the Bank to rectify inaccurate, incomplete or obsolete Data;
- right to request restriction of Data pending such a request being considered;
- right to withdraw consent at any time;
- right to ask the Bank to stop processing the Data;
- right to request deletion of Data (except where major overriding interests require the processing to continue);
- right to object to direct marketing, including profiling;
- right under applicable data protection laws, to request Data be transferred to the client or to another controller;
- right to ask the Bank for a copy of some or all of Data collected and processed about the client.

VIII. EXERCISING RIGHTS

The Client may exercise any of his/her rights in relation to his/her Data by writing to the following address: dataprotection.legal@heritage.ch. Please enclose with the signed letter a copy of your passport or identity card.

IX. SECURITY NOTE

The Bank has put in place appropriate technical and organisational measures at the earliest stages of the software ("*Data protection by design*") and implemented measures to ensure that, by default, only personal data, which are necessary for each specific purpose, are processed ("*Data protection by default*"). Furthermore, the Bank has in place necessary security measures to prevent unauthorised or unlawful access to the Data. As complete data security cannot be guaranteed for communication via e-mails, instant messaging, and similar means of communication, we recommend sending any particularly confidential information by an alternative secure means.

X. CHANGES TO DATA

The Bank is committed to keeping the Data accurate and up to date. Therefore, if the Data change, the Client shall inform the Bank of any change as soon as possible.

XI. ROLES AND RESPONSABILITIES

The table below shows the roles and responsibilities:

Roles	Responsabilities
Overall Data framework	Legal Department
Data processing	IT Department
Access profiles	IT Department
Data access and consultation	Legal Department
Data technical security	IT Department
Data correction and destruction	IT Department

October 2018