The Niche

Information on Data Protection under the Swiss Data Protection Act (DPA)

In the context of its business activities, The Niche SA (hereinafter also referred to as the "Company", "we" or "our") processes data relating to natural persons and legal entities (hereinafter "Personal Data"). Such Personal Data includes information about our clients (current and former), prospective clients, business partners and their employees, as well as any other individuals who interact with the Company.

The Company complies with applicable laws and regulations to ensure the protection and confidentiality of Personal Data. This document provides an overview of how we process Personal Data and outlines the rights of the individuals concerned.

1. Types of Personal Data Processed

Depending on the product or service provided, the Company collects in particular the following categories of Personal Data:

- Personal information such as full name, date and place of birth, nationality, address, gender, phone number, postal and email address, as well as information about family members or close associates such as the name of spouse/partner and/or children;
- Financial information, such as records of payments and transactions, information regarding the client's assets (movable and immovable), financial statements, liabilities, taxes, income, earnings, and investments;
- Tax residence and other tax-related documents and information, such as tax identification number;
- Professional information about the client, including job position and work experience;
- Knowledge and experience in the field of investments;
- Details of client interactions, products and services requested, and any powers of attorney granted;
- In some cases (where permitted by law), special categories of Personal Data, such as biometric data, political opinions and affiliations, health-related data, racial or ethnic origin, religious or philosophical beliefs, and, where legally allowed, data relating to criminal convictions or offences.

In certain cases, the Company may also collect the above information from public records, public authorities, or other third-party sources such as the custodian bank. Where relevant to the services provided to clients, the Company may also collect information about co-holders of cards or accounts, shareholders (including other stakeholders or beneficiaries), dependents or family members, representatives, and agents.

When a user accesses the Company's website (www.theniche.ch), data transmitted by their browser is automatically logged by our server (including date and time of access, name of the file accessed, data volume transferred, access status, user's browser, language and domain, IP address). Additional data will be collected through our website only with voluntary consent, for example during registration or inquiries.

The Company may use cookies, tracking technologies, and other tools (e.g., web beacons, pixels, gifs, tags, unique identifiers) to collect and process the above information through various channels, including email and the devices used to interact with the website. For details on the use of cookies and tracking technologies, please refer to our Cookie Policy available on the website.

2. Purpose of Data Processing and Legal Bases

The Company processes the aforementioned Personal Data in accordance with the provisions of the Swiss Federal Data Protection Act (DPA). Your Personal Data is always processed for a specific purpose and only to the extent necessary to achieve that purpose. The primary purposes for such data processing are as follows:

2.1. Fulfilment of Contractual Obligations

Data is processed to provide financial services within the framework of contracts concluded with clients or to carry out pre-contractual measures in anticipation of entering into such contracts. The specific purposes of data processing primarily depend on the particular service requested by the clients and may include needs assessments.

2.2. Compliance with Legal Obligations

The Company is subject to various legal obligations (such as the Financial Institutions Act, the Anti-Money Laundering Act, and the Financial Services Act) as well as regulations issued by the supervisory body to which the Company is affiliated (OSFIN) and FINMA, which may require the processing of Personal Data.

2.3. Pursuit of Legitimate Interests

Where necessary, we process data beyond what is strictly required for the fulfillment of our contractual obligations in order to pursue our legitimate interests or those of a third party, provided that such interests do not override the interests, rights, and fundamental freedoms of our clients. In addition to the examples below, we may obtain Personal Data from publicly available sources for the purpose of client acquisition:

- asserting legal claims and establishing a defense in case of litigation;
- ensuring IT security and the operation of the Company's IT systems;
- preventing and detecting criminal offences;
- video surveillance to prevent unauthorized access, collect evidence in the event of theft or fraud, or verify availability and deposits;
- measures for the security of buildings and premises (e.g., access control);
- measures to manage operations and further develop services and products.

Where the Company processes Personal Data in accordance with sections 2.1, 2.2, and 2.3, it is not necessary to obtain the data subject's explicit prior consent.

2.4. Specific Purposes

If the data subject has consented to the processing of Personal Data for specific purposes (e.g., analysis of trading activity for marketing purposes, etc.), the lawfulness of such processing is based on that consent. Consent granted may be withdrawn at any time.

3. Access to and Protection of Personal Data

Within the Company, access to data is granted only to employees who require it in order to fulfill contractual, legal, and regulatory obligations. Service providers and representatives (typically providers of banking, IT, logistics, printing, telecommunications, collection, consultancy, sales, and marketing services) who may be engaged by the Company may also receive data for these purposes, provided they comply with the applicable regulations on the processing of Personal Data.

With regard to the transfer of data to recipients outside the Company, it should first be noted that employees of The Niche are bound by confidentiality obligations concerning any facts and assessments related to clients of which they may become aware.

Under certain conditions, the Company may disclose information to third parties, such as:

- Public authorities and institutions (e.g., FINMA, supervisory bodies, audit firms, financial authorities, law enforcement agencies), provided that there are legal obligations to do so;
- Other financial service providers, similar institutions, and data processors to whom we transmit Personal Data in order to carry out our mandate (e.g., support/maintenance of data processing/IT applications, data storage, document processing, compliance and risk management services).

Appropriate technical and organizational measures have been implemented to prevent any unauthorized or unlawful access to the Personal Data provided by clients.

4. Transfer to a Third Country

Data may be transferred to countries outside Switzerland only if this is necessary for the performance of the agreed service (e.g., securities transactions), if required by law (e.g., reporting obligations under tax legislation), or if the client has given their consent. If service providers in a third country are used, they are required to comply with data protection standards equivalent to those applicable in Switzerland.

5. Data Retention Period

The Company retains Personal Data only for as long as necessary to fulfill the purpose for which it was collected or to comply with legal, regulatory, or internal policy requirements. Specific criteria are applied to determine appropriate retention periods based on the purpose of the data, such as proper accounting practices, maintaining the client relationship, defending against legal claims, or responding to regulatory requests. In general, the Company retains Personal Data for the duration of the relationship or contract, plus an additional ten years, reflecting the period allowed for initiating legal action following the termination of such relationship or contract. An ongoing or threatened legal or regulatory proceeding may result in retention beyond this period.

6. Data Protection Rights

6.1. General

Every data subject has the right to be informed about their data, the right to have it corrected or deleted, to restrict or object to its processing, and, where applicable, the right to obtain the transfer of such data. Within applicable limits, the right to lodge a complaint with a competent data protection authority is also granted.

Consent to the processing of Personal Data may be withdrawn at any time. Such withdrawal will only apply to future processing; any processing carried out prior to the withdrawal will not be affected.

The rights of access, withdrawal, or objection are not absolute and may not apply in certain circumstances or may be subject to exceptions (for example, to comply with legal obligations). We will respond to requests in accordance with applicable data protection laws. Additionally, when a data subject exercises their rights, we may first ask them to provide proof of identity. We may also request additional information if the request is unclear. If we are unable to fulfill the request, we will provide an explanation.

To exercise your rights, please use the contact details provided in section 11.

6.2. Right to Object to the Processing of Data for Marketing Purposes

In certain cases, we process Personal Data for direct marketing purposes. The data subject has the right to object at any time to the processing of their Personal Data for such purposes, including profiling to the extent that it is related to direct marketing.

If an objection is raised to the processing for direct marketing purposes, the Personal Data will no longer be processed for these purposes.

To submit an objection, please use the contact details provided in section 11.

7. Obligation to Provide Data

In the context of delivering our services, the data subject is required to provide the Personal Data necessary to enter into and carry out the mandate, and to fulfill the related contractual and legal obligations. Without such data, we are generally unable to enter into or execute a contract with our clients.

Specifically, anti-money laundering regulations require us to verify identity before initiating a business relationship. To enable us to comply with this legal obligation, data subjects are required to provide the necessary information and documents, and to promptly notify us of any changes that may occur during the course of the mandate. If the required information and documents are not provided, we are not permitted to deliver our services.

8. Use of Automated Decision-Making Processes

As a rule, the Company does not make decisions solely based on automated processes for the purpose of establishing or managing a business relationship. Should the Company use such processes in individual cases, it will provide separate notification to the extent required by law. A right to object will be granted under certain circumstances.

9. Profiling by the Company

In certain cases, we process client data automatically in order to evaluate specific personal aspects (profiling). Examples include:

- Legal obligations require us to adopt anti-money laundering, anti-fraud, and counter-terrorism financing measures, as well as measures against crimes that pose a threat to assets. In this context, data evaluations may also be carried out (e.g., in payment transactions);
- We may perform client profiling to comply with regulatory and contractual requirements (e.g., determining the client's investment profile).

10. Data Security

The Company implements appropriate technical measures (e.g., encryption, pseudonymization, logging, access controls, data backups, etc.) and organizational measures (e.g., staff instructions, confidentiality agreements, audits, etc.) to ensure the security of the information collected and processed, and to protect it against unauthorized access, misuse, loss, falsification, and destruction. Access to your Personal Data is granted only when strictly necessary.

However, it is generally impossible to completely eliminate security risks: certain residual risks are almost always unavoidable. In particular, since absolute data security cannot be guaranteed for communications via email, instant messaging, or similar means, we recommend sending confidential information through particularly secure channels.

11. Data Controller and Contact Information

The responsible unit is the Company's Data Protection Officer, who can be contacted at the following address:

THE NICHE SA
Corso Elvezia 9
6900 Lugano

Phone: +41 91 950 1540
e-mail: compliance@theniche.ch