Privacy statement for clients

I. Name and address of the responsible person and the data protection officer

The responsible person according to the General Data Protection Regulation (GDPR) is:
Consilium Treuhand AG, Austrasse 15, FL-9495 Triesen

The contact details of the operational data protection officer are as follows:
Tel.: +423 265 51 51
E-Mail: toendury@toendury.li

II. Data processing in general

1. Scope of the processing of personal data

The processing of personal data is limited to data that is required to operate a functional website and for the provision of content and services. The processing of personal data of our users is based on the purposes agreed with you or on a legal basis (GDPR). We only collect personal data that is necessary to implement and process our tasks and services or if you provide data voluntarily.

2. Your rights (rights of the persons affected)

You have the right to request information about any of your personal data we process. In particular, you have the right to request information about the purpose of the processing, the categories of personal data, the categories of recipients who will have access or were disclosed with your data, the duration periods for saving the personal data, whether there is a right to adjust/correct, erase, restrict or object, transmission of data[1], the source of your data if not collected through us and if we use automatic decision-making technologies including profiling.

Additionally, you have the right to revoke a previously granted consent to use your personal data at any time.

If you believe that the processing of your personal data is inconsistent or contradicts the applicable data protection laws you have the possibility to lodge a complaint with the data protection office.

III. Description and scope of data processing

1. Purpose of data processing

We process our clients' personal data for the following purposes:

- Activities pursuant to Article 2 of the Liechtenstein Professional Trustees Act (*Treuhändergesetz* – TrHG) in conjunction with the Liechtenstein Persons and Companies Act (*Personen- und Gesellschaftsrecht* – PGR), in particular:

  – Client mandate management (including administration of legal entities)

[1] As long as it does not cause a disproportionate effort to transmit these data

- Auditor functions (review)
- Compliance with statutory accounting requirements
- Correspondence

- Compliance with legal obligations, in particular:
  - PGR, TrHG, due diligence laws, tax legislation and treaties

2. Categories of data

The following categories of data are processed in our data directories pursuant to Article 4(1) of the GDPR for the purposes of our activities outlined under Section 1 above:

Data category	Data description	Data recipient
Client and address data	Name, company name, date of birth, home and/or business address, nationality, occupation, telephone number, e-mail address	external service providers (such as banks, asset managers, auditors) and public bodies (e.g. supervisory or tax authorities)
Identification information	Identity documents including copies of passports and official ID papers, utility bills, tax numbers, death certificates, authentication data, including specimen signatures	banks, asset managers
Due diligence documentation	Including contracting partners, identification of beneficial owners, business relationship profiles with background information about occupation and private situation (e.g. job and hobbies), World-Check data, checks pursuant to the Liechtenstein Due Diligence Act (DDA; S*orgfaltpflichtsgesetz – SPG*)	Banks, public bodies
Mandate information	Including company documents, bank documentation, correspondence, documents pursuant to the DDA, resolutions of governing bodies	No forwarding
Accounting data	Transactions and accounting information	Tax authorities (for domestic taxpayers)
Correspondence	Client orders, general	No forwarding
Legal entity information	Articles of Association, by-	No forwarding

	laws, certificates, mandate contracts, signing authorities	
Tax reporting data	Reports based on FATCA, the automatic exchange of information (AEOI) and the Liechtenstein Disclosure Facility (LDF)	Tax authorities

3. Legal basis

The data listed under Section 2 above will be processed

- on the basis of our contractual relationship with our clients (Article 6(1)(b) of the GDPR);
- in order to fulfil a legal obligation (Article 6(1)(c) of the GDPR);
- to carry out a task in the public interest or in the exercise of official authority (Article 6(1)(e) of the GDPR); or
- for the purposes of the legitimate interests pursued by the data controller or a third party (Article 6(1)(f) of the GDPR).

Processing for the purposes of our legitimate interests may include:

- Processing for the purpose of internal administration
- Evaluations
- Marketing
- Direct marketing
- Video surveillance
- Defending against unjustified claims
- etc.

4. Recipients of personal data

Clients' personal data will only be processed by us to carry out our contractual, statutory and regulatory obligations for the purposes listed under Section 1 above.

For these purposes, data may be shared with the following:

- Companies within our group of companies for the purpose of internal administration
- External services providers and offices:
  - Banks
  - Asset managers
  - Insurance companies
  - Lawyers
  - Auditors
  - Suppliers
  - Merchants
  - Transport companies
  - Subcontractors
  - Other cooperation partners
  - Associations
  - Public interest organisations in Liechtenstein and abroad
  - etc.

If we have statutory or regulatory obligations to fulfil, personal data may be sent in particular to the following:

- Public offices and authorities (e.g. supervisory authorities, courts)
- Tax authorities (including in the scope of AEOI and FATCA)
- Authorities of third countries or international organisations

5. Sharing data with third countries or international organisations

If we transfer clients' personal data to other countries, it is protected and transferred in accordance with the statutory provisions. Transmission of data outside of the European Economic Area is done with the following guarantees:

- The country to which we are transmitting the personal data has assured the European Commission of an appropriate level of protection of personal data.
- The recipient has signed a contract based on the Standard Contractual Clauses confirmed by the European Commission, undertaking to protect personal data.
- If the recipient is located in the USA, the recipient is a certified member of the EU-US Privacy Shield Framework.

Additional information about the protection of personal data when it is transmitted outside the European Economic Area can be provided on request.

6. Data sources

We collect data either directly (e.g. in meetings or through correspondence with clients; internal background and due diligence checks) or partially from third-party service providers.

Third-party service providers may include:

- Banks
- Asset managers
- Auditors
- Other intermediaries
- etc.

7. Storage periods

Personal data will be processed and stored for the duration of the business relationship within the framework of the statutory provisions. Once the business relationship has been terminated, these data are retained for 10 years on the basis of statutory provisions (PGR, DDA, Liechtenstein Civil Code [*Allgemeines bürgerliches Gesetzbuch* – ABGB]). Longer retention periods will be enforced only on the basis of statutory or contractual requirements to retain data or for the purpose of maintaining evidence within any applicable statutory limitation periods.

8. Automated decision-making (Article 22 of the GDPR)

No automated decision-making processes are applied to clients' personal data. Where such processes are used in individual cases, we inform the clients to the extent required by the law.

9. Necessity of the data (Article 13(2)(e) of the GDPR)

Provision of the data listed under Section 2 above is mandatory in order to allow us to offer our clients the services they require and fulfil our statutory obligations. In addition to possible statutory reporting obligations to the responsible supervisory authorities, failure to provide data will result in the non-establishment or termination of the business relationship.

IV. Data security

We use a common encryption technology SSL or TLS encryption programme in connection with the highest encryption levels that are supported by your browser. If a page on our website was/is being transmitted encrypted it is shown by the lock symbol in the address bar of your browser.

Additionally, we use appropriate technical and organizational security measures to protect your data from accidental or intentional manipulation, partial or complete loss, destruction, or to prevent unauthorized access by third parties. Our security measures are continuously upgraded according to the latest technological developments.