



FELDER SPRENGER+
PARTNER

DATA PROTECTION DECLARATION **FOR PARTNERS, CUSTOMERS AND CLIENTS**

Please note that this is a translation of our German Data Protection Declaration. In case of deviations, the German version shall prevail.

With this Data Protection Declaration, we would like to provide you with an overview of the manner in which we process your data and your rights in this connection according to the provisions of the European General Data Protection Regulation (hereinafter called "GDPR") and the Liechtenstein Data Protection Act (Datenschutzgesetz, hereinafter called "DSG"):

I. NAME AND ADDRESS OF THE DATA CONTROLLER AND THE DATA PROTECTION OFFICER

Data Controller within the meaning of the GDPR is:

Felder Sprenger + Partner AG
Landstrasse 158
9494 Schaan
Liechtenstein

T +423 230 20 90
office@fsp.li
www.fsp.li

Our Data Protection Officer, Sabrina Ann Rivera, can be reached using sabrina.rivera@fsp.li, T +423 230 20 90 or our postal address with the supplement "Data Protection Officer".

II. GENERAL INFORMATION CONCERNING DATA PROCESSING

1. Extent of the processing of personal data

Processing personal data is limited to the data necessary in order to provide a well-functioning web page as well as to provide our services. Processing personal data of our users only take place for the agreed purposes or on a legal basis within the meaning of the GDPR.

We only collect the personal data absolutely necessary to implement and process our duties and to provide the agreed services or data you have voluntarily disclosed.

2. Your data protection rights

You have the right to demand information on your personal data processed by us. In particular, you are entitled to demand disclosure regarding the purpose for which your data is collected, the categories of personal data collected, the categories of third party recipients, who have received or will receive your personal data as well as the storage period. Additionally, you have the right to rectification, deletion, restriction of the processing, objection, data portability (unless a disproportionate effort is incurred in the case of data portability), as well as to receive information on its origin, if not collected by us, and to be informed on automatic decision making including profiling.

You have the right to withdraw any given consent to use your personal data at any time.

If you are of the opinion that our processing of your personal data is in breach of applicable data protection law or that your statutory data protection rights have been infringed otherwise, you may file a complaint with the competent supervisory authority. In Liechtenstein, the Data Protection Office (www.datenschutzstelle.li) is the competent authority.

III. DESCRIPTION AND EXTENT OF DATA PROCESSING

1. Purposes of data processing

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

- Activities according to Art. 2 Trusteeship Act in connection with the Law of Persons and Companies, especially:
 - Mandate administration (incl. legal entity administration)
 - Auditor function (audit review)
 - Legal obligation to keep records
 - Correspondence
- Fulfillment of legal obligations, especially
- Persons and Companies Law, Trusteeship Act, Due Diligence Legislation, Tax Laws and Agreements (e.g. FATCA, CRS, Register of Beneficial Owners of Legal Entities (Vwbp), final withholding tax etc.)

2. Data Categories

In our data folder the following data categories according to Art. 41) GDPR are being processed in order to be able to fulfill our activities as mentioned in clause 1:

Data category	Description	Recipient	Origin	Sensitive data	Storage period
Personal and address data of natural persons	First name, last name, date of birth, place of birth, private and/or business address, nationality, telephone number, e-mail-address, tax identification number etc.	Employees, external agents (e.g. banks, asset managers, auditors) and public authorities (e.g. supervisory authorities or tax authorities)	Direct survey or via intermediaries	no	10 years
Identification data	Identification documents, e.g. passport copies, ID-copies, utility bills, tax identification numbers, death certificates, authentication documents such as signature specimens etc.	Employees, external agents (e.g. banks, asset managers, auditors) and public authorities (e.g. supervisory authorities or tax authorities)	Direct survey or via intermediaries	no	10 years
Due Diligence data (DDA/DDO)	Identification of the contracting partner, the beneficial owner, the recipient of distributions; business profiles including information on the personal and occupation background, origin of the assets, world-check data, due diligence investigations, PEP-check etc.	Employees, external agents (e.g. banks, asset managers, auditors) and public authorities (e.g. supervisory authorities or tax authorities)	Direct survey or via intermediaries, Internet, Pythagoras (World-Check)	no	10 years
Mandate Information	Mandat documents, bank documents, correspondence, due diligence documentation, tax data, resolutions etc.	Employees, external agents (e.g. banks, asset managers, auditors) and public authorities (e.g. supervisory authorities or tax authorities)	Direct survey or via intermediaries	no	10 years
Bookkeeping/ accountig data	Transaction information, book-keeping information, recipients of payments, description of activities, VAT number, currencies, amounts etc.	Employees, external agents (e.g. banks, asset managers, auditors) and public authorities (e.g. supervisory authorities or tax authorities)	Direct survey or via intermediaries, banks	no	10 years

Correspondence	Client instructions, correspondence with beneficiaries, settlors, shareholders, recipients of distributions, bodies, protectors, general correspondence etc.	Employees, external agents (e.g. banks, asset managers, auditors) and public authorities (e.g. supervisory authorities or tax authorities)	Direct survey or via intermediaries	no	10 years
Legal entity data	Articles/statuts, by-laws, beneficiary regulations, letter of wishes, declarations of renunciations, certificates, contracts, documentation of signatories etc.	Employees, external agents (e.g. banks, asset managers, auditors) and public authorities (e.g. supervisory authorities or tax authorities)	Direct survey or via intermediaries	no	10 years
Tax reporting information	FATCA-, AIA-, LDF-, ASTA-reportings, Register of Beneficial Owners of Legal Entities (VwbP)	Employees, external agents (e.g. banks, asset managers, auditors) and public authorities (e.g. supervisory authorities or tax authorities)	Direct survey or via intermediaries	no	10 years

3. Legal Basis

The data mentioned in 2 is processed:

- based on contractual measures with our clients (Art. 6 Para 1 lit. b GDPR)
- in order to fulfill legal duties (Art. 6 Para 1 lit. c GDPR)
- due to public interest (Art. 6 Para 1 lit. e GDPR)
- to protect legitimate interest by us or third parties (Art. 6 Para 1 lit. f GDPR)

Processing activities to protect our legitimate interest can be:

- processing for internal administrative purposes
- evaluations
- marketing purposes
- rejection of unjustified claims

4. Video conference

In order to be able to offer video conferences, Felder Sprenger + Partner AG uses the functions of "Zoom", which is a service of Zoom Video Communications, Inc., based in San Jose, California, USA.

Various data are processed when using Zoom. The data processed also depends on the data you provide. To be able to participate in the video conference, you must at least provide your e-mail address and your name. In order to establish a connection, improve the user experience and also to carry out anonymous analysis to improve the services of Zoom, additional technical data such as IP-address, device type, operating system type etc. are processed. Further information can be found in Zoom's data protection declaration at <https://zoom.us/de-de/privacy.html>

You may have the option of using the chat functions in our video conference. In this respect, the text entries you make will be processed in order to display them during the video conference. In order to enable the display of video and audio, the data from the microphone of your end device and any video camera of the end device are processed accordingly during the duration of the meeting. You can switch off the camera or mute the microphone yourself at any time using the "Zoom" applications.

It is possible to record the video conference, but this function is usually not used by Felder Sprenger + Partner AG. Should it be the case, you will transparently be informed before the video conference begins and -if necessary- you will be asked for your consent. The fact that the recording function is used is additionally shown while using Zoom.

There is no automated decision making according to Art. 22 GDPR. The legal basis for using Zoom is Art. 6 Para. 1 lit. b GDPR.

5. Recipients of personal data

Personal data of our clients are only processed if required in order to comply with our contractual, statutory and supervisory obligations for the purposes mentioned in Clause 1.

Additionally, the following persons may receive data:

- Banks
- Asset managers
- Insurances
- Lawyers
- Auditors
- Suppliers
- Distributors
- Transport companies
- Other cooperation partners
- Representative associations
- Public interest establishments
- IT-service providers

If we have to fulfill legal or supervisory duties, the following bodies may receive personal data:

- Authorities and public bodies (e.g. supervisory authorities, courts)
- Tax authorities (i.a. in regards to the exchange of information in connection with CRS, FATCA etc.)
- Authorities of third countries and international organizations.

6. Transfer of personal data to third party states or international organizations

Data is only transferred to countries outside the European Economic Area (so-called third countries) within the context of adequacy decisions of the European Commission or if this is necessary for the implementation of pre-contractual measures or the performance of a contract, if you have given us your explicit consent (e.g. within the context of specific services), if the transfer is necessary for significant reasons of public interests or is stipulated by law.

If we transfer personal data from our clients to another country, the data will be protected and transferred in accordance with the legal provisions. A transfer of data outside of the European Economic Area only take place if the following can be guaranteed:

- The country to which personal data is sent provides an adequate level of protection according to the European Commission;
- The recipient has a signed a contract based on the “model contract terms” of the European Commission, which commit the recipient to protect the personal data
- If the US-recipient is a certified member of the EU-US-privacy shield

7. Data Origin

Data is either gathered directly (e.g. during meetings or by means of correspondence with clients; internal background check and due diligence investigations) and partly from third party providers.

Third party agents can be:

- Intermediaries
- Lawyers
- Banks
- Asset Managers
- Other contact persons

8. Storage period

Personal data are processed and stored during the active business relationship on the basis of legal obligations. After the end of the business relationship the data is retained until expiration of the statutory retention period of 10 years (PGR, SPG, ABGB). Further processing and a longer storage period only may be conducted for reasons of legal or contractual retention periods or for reasons of preservation of evidence within the limitation periods.

9. Automated decision making (Art. 22 GDPR)

No automated decision making with personal data of our clients takes place. Should this take place in particular cases, we will inform our clients accordingly.

10. Necessity of the data (Art. 13 Para 2 lit. E GDPR)

In order to be able to offer you as our client the desired service to the full extent and taking into account statutory regulations, we require the data mentioned in Clause 2. Not releasing the required data results in possible statutory reporting obligations to the relevant bodies, not being able to enter into a business relationship or the termination of our business relationship.

IV. DATA SECURITY

We use technical and organizational security measures, in order to protect your data against accidental or intentional manipulation, partly or total loss, destruction or access by unauthorized third parties. Our safety measures are constantly improved according to technological developments.

V. VALID VERSION

This is the currently valid Data Protection Declaration as of November 2022.

Due to the continued development of our website and associated services or organizational modifications within our law firm or on the grounds of amended legal or regulatory requirements, it may become necessary to amend this Data Protection Declaration. You can access and print out the respective current Data Protection Declaration on our website at any time.