schreiber maron sprenger
Versicherungsbroker

Data Processing Policy

Schreiber Maron Sprenger AG | Vaduz

Valid from: 01.09.2023

Table of contents

1. General provisions

For the sake of readability, gender-specific differentiation is not used throughout the document. All references to persons apply to all genders in the interests of equal treatment.

1.1. Legal basis

This Data Processing Policy has been drawn up on the basis of the following laws and ordinances:

- The European Union's General Data Protection (GDPR) of 27 April 2016 (version dated 4 May 2016)
- Data Protection Act (DSG) of 25 September 2020 (version dated 1 September 2023)
- Data Protection Ordinance (DPO) of 31 August 2022 (version dated 1 September 2023)
- Personal and Company Law (PGR) of 20 January 1926 (version dated 1 August 2022)

1.2. Aim of the Data Processing Policy

The Data Processing Policy ensures that the personal and fundamental rights of persons whose personal data is processed at Schreiber maron Sprenger AG are protected in accordance with the statutory provisions. The Data Processing Policy describes in particular the data processing and control procedure and mention which documents exist concerning the planning, implementation and operation of the data collection.

1.3. Purpose of data processing

Schreiber Maron Sprenger AG is a provider of tailor-made insurance and risk solutions. It offers services in the field of occupational pension plans, personal, property and liability insurance, as well as risk management. In order to be able to offer the customer tailored solutions and maintain correspondence with them and the insurers, the processing of personal data is essential for order fulfilment.

1.4. Responsible data protection office

The **internal** officer responsible for data protection issues and contact for questions is:

Jan Müller
Managing Director

Schreiber Maron Sprenger AG
Holy Cross 42
9490 Vaduz, Liechtenstein

Tel. +423 237 57 77
E-mail j.mueller@schreibermaronsprenger.li

2. Information system structure

2.1. Printers and postal delivery

The printers are provided and maintained by Witzig The Office Company AG, in 8500 Frauenfeld, Switzerland. Liechtensteinische Post AG, in 9494 Schaan, Liechtenstein, is responsible for postal delivery.

2.2. Components of the information system

2.2.1. Corporate management

Overall responsibility for data protection lies with the Executive Board. This responsibility is not transferable.

2.2.2. E-mail, Internet/intranet and telephone

Internet access for business purposes is configured for all customers. An individual e-mail account and a direct line are set up for each employee. The transitions from the internal to the external network are protected by a firewall. Only selected employees of Schreiber Maron Sprenger AG registered at UMB AG, 6330 Cham, Switzerland, can access the system of Schreiber Maron Sprenger AG externally using a code.

Private use of the infrastructure/e-mails is tolerated to a limited extent and must be done outside working hours or during breaks.

2.2.3. HR management

Internally, one employee is entrusted with the tasks of HR management.

2.2.4. Document management

The data and documents are stored centrally on the servers of UMB AG and Microsoft and are launched using PowerApp (brokers) and Office365. Access authorisation to specific data and documents is granted according to the function and role of an employee.

2.2.5. IT operations

The IT area is handled by the outsourcing partner UMB AG. UMB AG provides the servers on which the applications, data and documents of Schreiber Maron Sprenger AG are stored. The insurance broker software is supplied and maintained by Brokinsoft SA, in 1950 Sion, Switzerland. These partners confirm by signing a contract that they comply with data protection regulations for themselves and their employees. IT support is provided by Qualibroker AG, in 8048 Zurich, Switzerland.

Employees can access the data on the servers of UMB AG that they need to carry out their activities via their computer (client). All data is regularly stored as a backup by UMB AG and archived by both UMB AG and Schreiber Maron Sprenger AG.

Both the firewall and the antivirus program must be regularly checked and kept up to date by UMB AG.

In addition, Qualibroker AG operates a customer portal. Use of the customer portal requires a separate user agreement between the customer and Qualibroker AG.

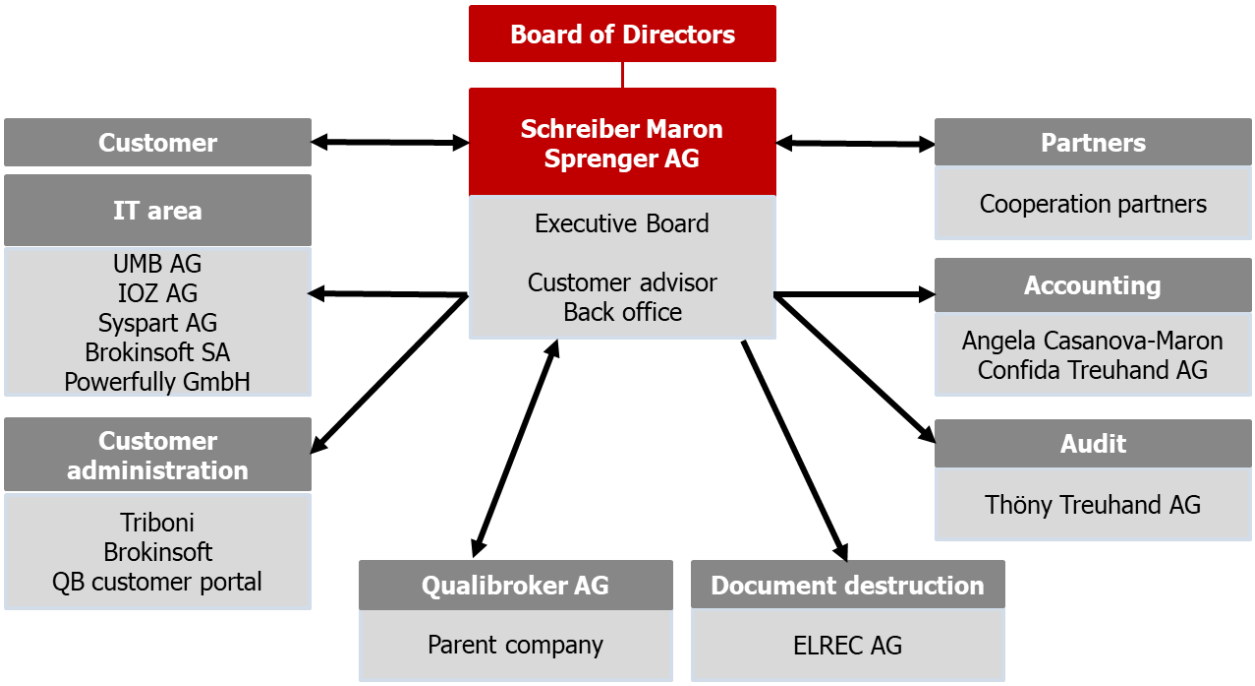
Promacx AG, in 3011 Bern, Switzerland, is responsible for web hosting.

2.2.6. Cookies

The following cookies are used on the website of Schreiber Maron Sprenger AG: Google Ads, Google Analytics, Facebook Marketing and Craft Cookie.

2.3. Interfaces

The diagram below shows the data and document interfaces of Schreiber Maron Sprenger AG to the outside world. A list of interfaces and an overview of suppliers and outsourcing relationships are maintained internally.



The personal data processed by Schreiber Maron Sprenger AG in the context of its activity as an insurance broker comprises data disclosed by the policyholder, insurer and insured party as well as data that is publicly available. As part of its duties as an employer, Schreiber Maron Sprenger AG processes personal data that it obtains from employees and applicants.

In order to obtain quotes for customers and take out insurance, it is necessary for customer data to be forwarded to the insurance partners of Schreiber Maron Sprenger AG for order fulfilment.

IT was outsourced to UMB AG. Within the scope of their activities, Syspart AG, in 8810 Horgen, Switzerland, IOZ AG, in 6210 Sursee, Switzerland, Office365, Brokinsoft SA, in 1950 Sion,Switzerland, and Powerfully GmbH, in 8307 Effretikon, Switzerland, have access to electronically recorded customer and employee data via the Qualibroker customer portal

Ms Angela Casanova-Maron, in 7013 Domat/Ems, Switzerland, and Confida Treuhand, Unternehmens- und Steuerberatung AG, in 9490 Vaduz, Liechtenstein, have been mandated with accounting and Thöny Treuhand AG, in 9495 Triesen, Liechtenstein with the audit. As a result of their work, they will be given access to the business documents of Schreiber Maron Sprenger AG.

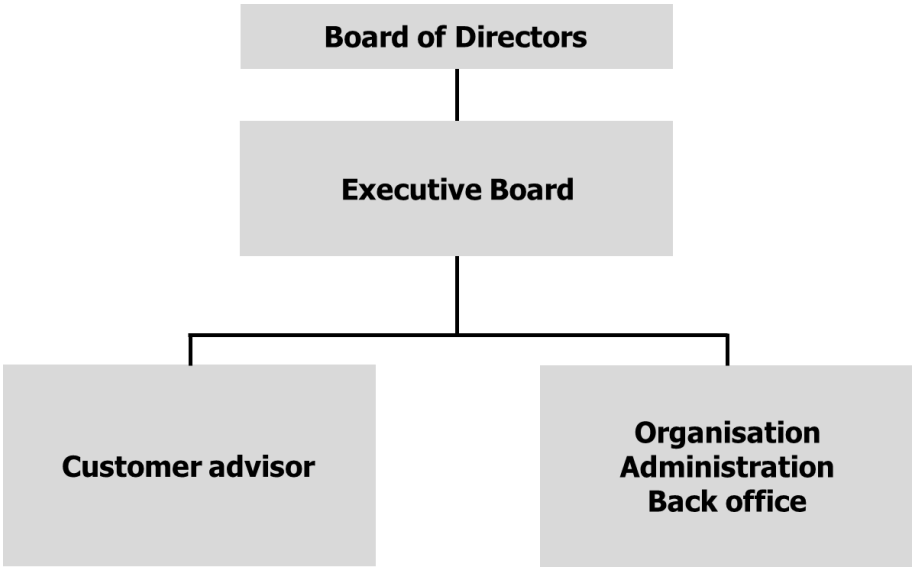
ELREC AG, in 9492 Eschen, Liechtenstein, is used to destroy documents containing customer and employee information in accordance with data protection regulations.

Schreiber Maron Sprenger AG works closely with its parent company in Switzerland, Qualibroker AG. To enable this collaboration, individual employees are also granted authorisation to process the customer data of the respective company (restricted to individual persons in administrative tasks such as accounting, IT support or similar).

3. Entities involved

3.1. Organisational areas of Schreiber Maron Sprenger AG

Overall responsibility for data protection lies with the Executive Board. This responsibility is not transferable.



4. User and data access

4.1. Users

All employees of Schreiber Maron Sprenger AG are users of the IT system and are able to process data. The access authorisations of all employees are documented and granted depending on their function and role.

Schreiber Maron Sprenger AG has guidelines on the use of IT and telecom infrastructure.

4.2. User management

User management is carried out by the IT coordinator at Qualibroker AG (outsourcing of IT support). The management of Schreiber Maron Sprenger AG is responsible for defining the IT access rights of the individual employees.

4.3. Cancellation of access authorisation

Users are entitled to access the data for as long as and to the extent that they need it to carry out their activities. In the event of departure or change of duties within the company Schreiber Maron Sprenger AG, the access authorisation shall be revoked and the access authorisations required for any new area of responsibility shall be reissued.

4.4. User training

The users of the IT system provided by UMB AG are trained in various ways in the area of data protection and application technology.

Every employee is made aware of the data protection provisions in the company in the employment regulations and signs to receive them. Employees receive regular training in the area of data protection. The training status of each employee is documented.

4.5. Instruction/directives

Data processing is governed by directives, regulations and guidelines. These are regularly updated by the relevant authority.

4.6. Processes

The data in the information system of Schreiber Maron Sprenger AG is collected, processed and passed on according to defined processes. Details on the processes can be found in the respective process descriptions. Details of the processes can be found in the respective process descriptions and are intended for internal use.

5. Data processing/data categories

5.1. Data origin

The personal data processed by Schreiber Maron Sprenger AG comprises data disclosed by the policyholder, insurer, insured persons or authorised third parties as well as publicly accessible data. No data is obtained from other third parties.

5.2. Categories of processed data

The main data categories that Schreiber Maron Sprenger AG processes in the system or stores on paper are as follows:

- Customer data (e.g. name, address, date of birth, gender, nationality, credit rating data)
- Data from applications, including the associated supplementary questionnaires (e.g. information provided by the applicant about the insured risk, answers to questions, expert reports, information provided by the previous insurer about the claim experience to date)
- Data from contracts with insurers (e.g. contract duration, insured risks, benefits, data from existing contracts)
- Debt collection data (such as the date and amount of premiums received, outstanding amounts, reminders, credit balances, payment details) and
- Any claims data (e.g. damage reports, investigation reports, invoices, data relating to injured third parties)

6. Data archiving

Schreiber Maron Sprenger AG has internal policies regarding document and data storage.

6.1. Archiving obligation

Documents that are subject to archiving are archived for the duration required by law and protected against changes and unauthorised access.

6.2. Retention period and deletion

The statutory retention period of ten years generally applies to the storage of business documents (Art. 1059 para. 1 PGR). If the business documents are stored electronically or in a similar manner, it must be possible to make them legible again during this time (Art. 1059 para. 3 and Art. 1060 para. 2 PGR).

Unless there is a statutory retention obligation, personal data will be retained for as long as it is necessary for the purpose for which it was collected. Then the data will be deleted.

7. Technical and organisational measures

7.1. Access control

Access to the office building of Schreiber Maron Sprenger AG is secured with a key system. Access to the offices in the building is also only possible by entering a code. Visitors must ring the bell at the reception so that access can be granted. Visitors must be accompanied at all times on the premises.

7.2. Data carrier control

Information technology measures enable only authorised persons to process data on the electronic data carriers.

Hard disks, state solid discs and other data carriers that are permanently installed with data processing systems for normal use may not be removed from the systems except for the purpose of disposal or repair. Furthermore, IT resources intended for stationary use may not be removed from the premises of Schreiber Maron Sprenger AG, except for the purpose of disposal, sale, migration or repair.

Data storage media must be irretrievably erased and, if possible, shredded before disposal.

Documents with customer-relevant data are destroyed by shredding or disposal (ELREC AG).

7.3. Transport control

Particularly sensitive data sent by e-mail is protected using server-to-server encryption.

SIM cards, flash memory, USB sticks and other data carriers intended for mobile use must be supervised and stored securely outside Schreiber Maron Sprenger AG. Mobile data storage media must be encrypted if technically possible.

Documents shredded by ELREC AG are stored and transported in locked containers until their actual destruction.

7.4. Disclosure control

The data subject must have consented to the disclosure of the data or it must be possible to assume consent in the circumstances. Sensitive data may only be passed on in encrypted form. Data transfers are logged. It must always be checked whether the person making the enquiry is entitled to information.

Persons authorised to provide information are stored in the insurance broker software. These are reviewed annually by the customer as part of the annual appraisal.

7.5. Memory control

Unauthorised entries, changes or deletions from the memory are prevented by access and authorisation control (e.g. user name/password) and by the IT applications. Regularly updating operating systems and applications minimises malware attacks. Regular backups are taken to protect sensitive data from loss.

7.6. Access control

Access to the information system of Schreiber Maron Sprenger AG is only possible with the corresponding authentication data. Access data is defined for each employee. Every employee receives this on their first day of work.

All passwords must be changed in a predefined intervals by the system. It is not allowed to set the same password for the same user twice in a row. If the login details are entered incorrectly several times, access to the information system is blocked and must be reactivated manually by the IT coordinator.

The system is protected by a firewall against use by unauthorised persons outside Schreiber Maron Sprenger AG. Security is monitored on an ongoing basis as part of IT security measures.

7.7. Input control

Unauthorised data entry into the memory must be prevented and it must be possible to subsequently check which personal data was entered at what time and by whom in the systems. For this reason, all entries and changes are continuously monitored and logged for reasons of system security and data integrity.

7.8. Measures in the area of end devices

Every employee receives a personal password for computer access on their first day of work. This password must be kept strictly confidential and must not be disclosed to third parties. The use of all software or the entire operating system of Schreiber Maron Sprenger AG outside the IT resources owned by Schreiber Maron Sprenger AG is only possible with the express permission of Schreiber Maron Sprenger AG. When leaving the workstation, employees are instructed to block access to the end device.

7.9. Separation of test and production servers

In order to test new software modules, data is copied to a test server. All tests are carried out on the test server and only with the data that is on the test server.

7.10. Data security breaches

If data security breaches are noticed, the direct line manager and the internal officer responsible for data protection issues must be notified immediately. Thereafter, the reporting obligation pursuant to Art. 33 and 34 GDPR is met. A process diagram has been created for internal use.

All breaches of data security are listed in a register. The following information is recorded:

- Date of incident and/or discovery of incident
- Who reported the incident
- What happened
- Whether Schreiber Maron Sprenger AG as controller or processor is affected
- Assessment of the risk to the privacy and fundamental rights of the data subject(s) affected by the data security breach
- To whom reports of the incident were made and the name and date of the report document
- Causes and effects of the incident
- Which data has been recovered – which of these manually
- How the restoration was accomplished and by whom it was performed
- What measures have been taken
- Responsible person

7.11. Working from home

Schreiber Maron Sprenger AG offers the opportunity to work from home or another location on a voluntary basis. It has been contractually agreed (employment regulations) that data security must be guaranteed at all times and in all locations. In particular, no

- physical documents are taken home and
- documents can be printed out at home on private devices.

Employees working from home are obliged to ensure that business secrets are protected and that family members and third parties cannot gain access to business data. If these requirements are not met, the option of working from home ends.

8. Rights of data subjects

A natural person who can be identified on the basis of the personal data processed by the Schreiber Maron Sprenger AG is a data subject. Schreiber Maron Sprenger AG processes personal data on the one hand as a processor of customer data and on the other hand as a controller for the processing of data of partners, employees and suppliers. In the first case, the customer is the controller. The rights of data subjects listed here must be asserted against the respective controller.

8.1. Information obligation when collecting personal data

In accordance with Art. 13 and 14 GDPR, Schreiber Maron Sprenger AG is obliged to inform its customers about the collection of personal data where it acts as data controller.

8.2. Right to information

Pursuant to Art.15 of the GDPR, every person has the right to request information from the controller as to whether data relating to them is being processed, what data is available about them, where this data comes from, the purpose for which it is being processed, to whom the data is being disclosed, what categories of data are available and for how long the data is being stored.

The request for information may be sent in writing together with a copy of the identity card or passport to the contact address of the controller. In the case of particularly complex applications, a cost contribution of up to a maximum of CHF 300.00 may be required.

8.3. Right of access and right to rectification

Data subjects have the right to see their personal data processed by the controller. If incorrect information is stored about you despite efforts to ensure that your data is accurate and up to date, it will be corrected at your request in accordance with Art. 16 GDPR. The data subjects shall be informed of this after the rectification.

8.4. Right to deletion

Insofar as the controller is not obliged or entitled to retain some of the personal data under applicable laws and regulations, data subjects have the right to have their data erased from the Controller's system in accordance with Art. 17 GDPR.

8.5. Right to restriction of processing

Subject to the conditions set out in Art. 18 of the GDPR, data subjects have the right to obtain from the controller restriction of processing.

8.6. Notification obligation in connection with rectification or deletion of personal data or restriction of processing

In accordance with Art. 19 GDPR, Schreiber Maron Sprenger AG notifies all recipients to whom personal data has been disclosed of any rectification or erasure of personal data or restriction of processing, unless this proves impossible or involves disproportionate effort. The Schreiber Maron Sprenger AG shall inform the data subject about these recipients if the data subject requests so.

8.7. Right to data portability

According to Art. 20 GDPR, data subjects have the right to receive the personal data concerning them which they have provided to a controller and to transmit it to another controller without hindrance from the controller to which the personal data have been provided.

8.8. Right to object

If the processing of data is not absolutely necessary for the fulfilment of a contract or if the controller is not obliged or entitled to the processing of data on the basis of applicable laws and regulations, data subjects may object to such processing at any time with effect for the future in accordance with Art. 21 of the GDPR.

8.9. Right to withdraw consent

Any consent to data processing that has been granted to the scribe Maron Sprenger AG can be revoked in accordance with Art. 7 GDPR. Revocation is as easy as granting consent.

8.10. Right to lodge a complaint

Data subjects have the opportunity to lodge a complaint with the competent data protection authority in the event of a violation of their rights.

9. Final provisions

9.1. Amendments to the Policy

The Data Processing Policy is updated on a regular basis. Its may be amended at any time. Changes must be made in writing and must be approved by the Chair of the Executive Board and the office responsible for data protection.

9.2. Approval

This Data Processing Policy has been approved by the management of Schreiber Maron Sprenger AG and enters into force on 1 September 2023.

Jan MüllerRoger Kälin
Managing Director

Member of the Executive Board