qualibroker

Data processing regulations

Qualibroker AG | Zürich

Valid from: 21/06/2019

qualibroker

Contents

1. General provisions

To improve the readability of the text, no distinction between genders has been made in this document. All terms used to denote persons refer equally to all genders.

1.1. Legal bases

These processing regulations have been drawn up based on the following laws and regulations:

- European Union General Data Protection Regulation (GDPR) of 27 April 2016 (version dated 4 May 2016)
- Swiss Federal Act on Data Protection (FADP) of 9 June 1992 (as at 1 January 2014)
- Draft of the Federal Act on Data Protection (D-FADP) in accordance with the resolution by the Federal Assembly of 15 September 2017
- Ordinance to the Federal Act on Data Protection (DPO) of 14 June 1993 (as at 16 October 2012)
- Code of Obligations (CO) of 30 March 1911 (as at 1 April 2017)

1.2. Objective of the processing regulations

The processing regulations will be used to ensure that the privacy and fundamental rights of persons whose personal data is processed by Qualibroker AG are protected as required by law. The processing regulations define the data processing and control procedures used, and specify the documents created for the planning, implementation and performance of data collection activities.

1.3. Purpose of the data processing

Qualibroker AG is a provider of tailor-made insurance and risk solutions. It offers services in the field of occupational pension provision, personal, property, liability and other non-life insurance, and risk management. The processing of customer data is essential in order to offer tailor-made solutions and to enable correspondence with customers and insurers.

1.4. Data controllers

Data protection officer:

Urs Thalmann
Managing director

Qualibroker AG
Baslerstrasse 52
CH-8048 Zurich

Tel. +41 43 311 21 51
Email urs.thalmann@qualibroker.ch

EU representative:

Jan Müller
Managing director

Schreiber Maron Sprenger AG
Heiligkreuz 42
FL-9490 Vaduz

Tel. +423 237 57 77
Email j.mueller@schreibermaronsprenger.li

2. Structure of the information system

2.1. Information system elements

2.1.1. Corporate management

The Executive Board has overall responsibility for data protection. This responsibility cannot be delegated.

2.1.2. Email, internet/intranet and telephone

Internet access for business use is configured on all clients. An individual email account and a direct line are set up for each employee. A firewall protects transfers from the internal network to an external network. Only selected employees of Qualibroker AG are able to access the Qualibroker AG system from external locations using a code.

Only very limited personal use of the equipment/email is tolerated and such use must take place outside of working hours or during breaks.

2.1.3. HR management

An internal employee is entrusted with HR management activities. An external recruitment company is engaged as needed for new appointments.

2.1.4. Document management

Data and documents are stored on servers belonging to an outsourcing partner and can be accessed by employees of Qualibroker AG via the cloud and a document management system. Access permissions for specific data and documents are granted based on an employee's function and role.

2.1.5. IT operation

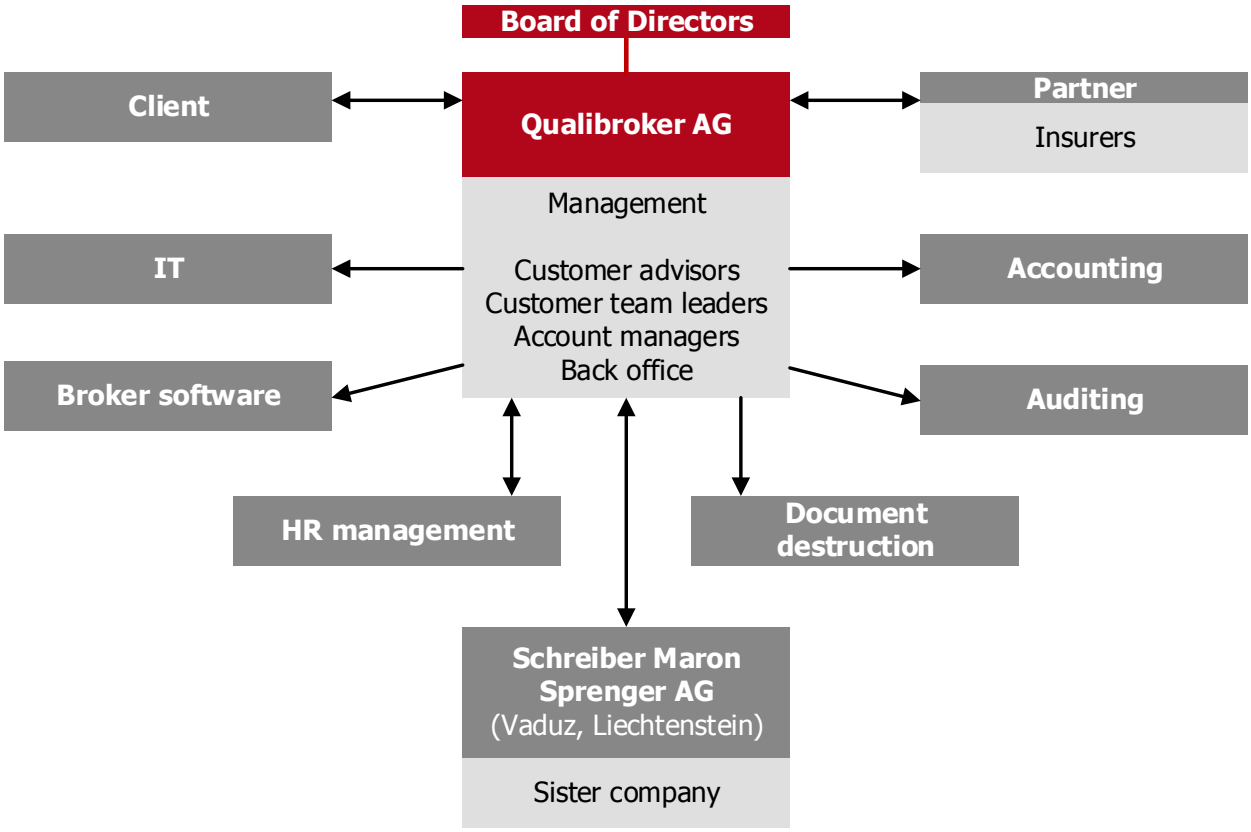
The operation of IT systems is outsourced to a partner. The servers on which applications, data and documents used by Qualibroker AG are stored are provided by this partner. The insurance broker software is supplied and maintained by a software specialist. These partners sign a contract confirming that they and their employees comply with data protection requirements.

Employees can use their computer (client) to access data on the servers that they require to perform their work. The outsourcing partner performs a regular back-up of all data, which is then archived both by the partner and by Qualibroker AG.

The outsourcing partner is responsible for regularly checking and updating the firewall and anti-virus software.

2.2. Interfaces

The graphic below shows the external data and document interfaces at Qualibroker AG. A list of interfaces and an overview of supplier and outsourcing relationships are maintained internally.



The personal data processed by Qualibroker AG as part of its activities as an insurance broker includes data provided by policyholders, insurers and insured parties, as well as publicly accessible data. As part of its activities, Qualibroker AG processes personal data obtained from employees, applicants and the recruitment company that may be engaged to provide HR management services.

In order to obtain quotes for clients and conclude insurance contracts, Qualibroker AG must share customer data with its insurance partners.

The outsourcing of IT means that during maintenance on the insurance broker software and provision of the document management system, electronic customer and employee data is editable by the outsourcing partner involved in these tasks.

Payroll accounting and the preparation of Qualibroker AG's financial statements are performed by a fiduciary company. Another fiduciary company is responsible for auditing. Both of these companies have access to business documents at Qualibroker AG due to the nature of their work.

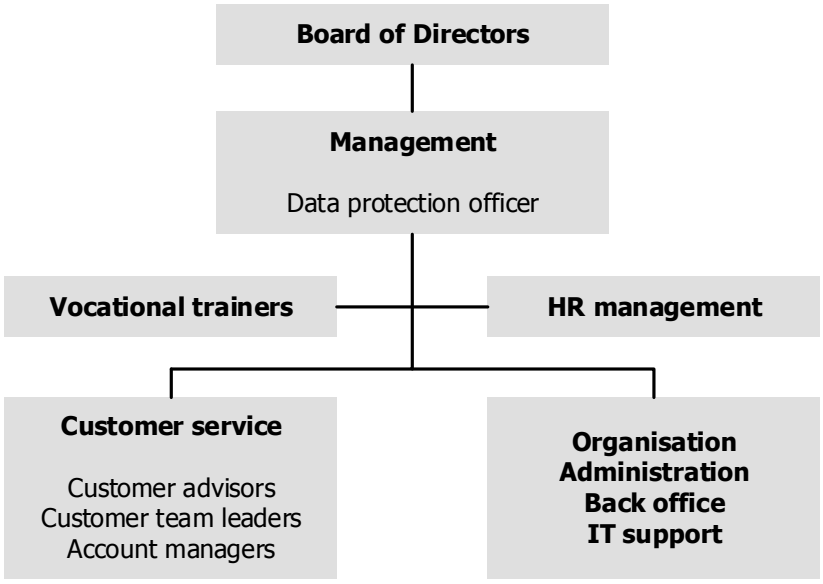
Qualibroker AG engages a specialist company to destroy documents containing customer and employee information in accordance with data protection requirements.

Qualibroker AG works closely with its sister company in Liechtenstein, Schreiber Maron Sprenger AG. To facilitate this collaboration, employees of each company generally also have edit authorisation for customer data of the sister company.

3. Parties involved

3.1. Organisational units of Qualibroker AG

The management has overall responsibility for data protection. This responsibility cannot be delegated. The internal data protection officer advises the company on implementing and complying with data protection requirements and performs the relevant checks. They are also the internal and external point of contact for questions relating to data protection in the company.



4. Users and access to data

4.1. Users

All employees of Qualibroker AG are users of the IT system and can edit data. All employees' access permissions are documented and granted based on the employee's function and role.

Qualibroker AG maintains regulations governing the use of the IT and telecommunications infrastructure.

4.2. User administration

The internal IT coordinator is responsible for user administration. Corporate management defines IT access rights for individual employees.

4.3. Revocation of access authorisations

Users are authorised to access the data for as long as necessary and to the extent necessary for their work. When users leave the company or change role within Qualibroker AG, their access authorisations will be revoked and new authorisations will be granted as necessary for the new role.

4.4. User training

Users of the IT systems provided by the outsourcing partner will receive various training on data protection and use of the systems.

The employment regulations inform all employees of the data protection requirements within the company, and employees sign to confirm receipt of these regulations. Employees receive regular training on the subject of data protection. The training received by each employee is documented.

4.5. Instruction

User guides exist for every application. Data processing rules are set out in instructions, regulations and guidelines. These documents are updated by the responsible individuals on a regular basis.

4.6. Processes

Qualibroker AG is certified to ISO 9001:2015. This means that defined processes are in place for the collection, processing and disclosure of data in the Qualibroker AG information system. Details of the processes can be found in the relevant process descriptions. These documents are easy to find via the process map on the Qualibroker AG intranet and are intended for internal use.

5. Data processing/data categories

5.1. Source of data

The personal data processed by Qualibroker AG includes data provided by policyholders, insurers, insured parties and authorised third parties, as well as publicly accessible data. No data is obtained from other third parties.

5.2. Categories of data processed

The key categories of data processed in Qualibroker AG's system or recorded on paper are as follows:

- Customer details (e.g. name, address, date of birth, gender, nationality, creditworthiness)
- Data from applications, including the corresponding supplementary questionnaires (such as applicant information on the insured risk, answers to questions, expert reports, information from the previous insurer on previous claims)
- Data from contracts with insurers (e.g. contract term, insured risks, cover, data from existing contracts)
- Collection data (e.g. date and amount of premiums received, outstanding amounts, reminders, credit, payment information)
- Any loss data (e.g. claims notices, investigation reports, accounting records, data on third parties that have suffered damage)

5.3. Registration of data files with the FDPIC

The statutory regulations do not require the data files processed by Qualibroker AG to be registered with the Federal Data Protection and Information Commissioner (FDPIC). As a holder of contact information and contracts with suppliers and outsourcing partners, and data files for its own HR management purposes, according to Art. 11a para. 5(a) FADP and Art. 4 para. 1(a) and (g) DPO, Qualibroker AG is not required to report its files.

Qualibroker AG processes other customer data files on behalf of these customers. The customer retains ownership of this data and is thus responsible for any registration with the data protection office.

6. Archiving of data

Qualibroker AG has internal regulations on the retention of documents and data.

6.1. Archiving obligation

Documents that must be archived are archived for the period stipulated by law and protected against changes and unauthorised access.

6.2. Retention period and deletion

The statutory retention period of 10 years applies to business documents (Art. 958f para. 1 CO). If business documents are stored in an electronic or similar form, they must be able to be made readable again throughout this period (Art. 958f para. 3 CO).

If there is no statutory retention obligation, personal data will be retained for as long as it is needed for the purpose for which it was collected. After this, it will be deleted.

7. Technical and organisational measures

7.1. Access control

Entry to Qualibroker AG office buildings is managed using a badge/key system. Offices in the building can also only be accessed by entering a code or using a key. Visitors must always ring the bell and report to reception so that access can be granted. Visitors must always be accompanied while on the premises. Rooms with technical equipment for data transmission and storage, such as servers, are secured with locking or entry systems and can only be accessed by a specific group of people.

7.2. Data media control

Technical measures are in place to ensure that only authorised persons can edit data on electronic storage devices.

Hard drives, solid state drives and other data media that are permanently installed in data processing systems during ordinary use may not be removed from the systems, except in the case of disposal or repair. Furthermore, IT resources designed for stationary use may not be removed from Qualibroker AG premises, except in the case of disposal, sale, migration or repair.

Data storage media must be permanently erased, and if possible shredded, prior to disposal.

Documents containing customer-related data are destroyed in a document shredder or by the relevant outsourcing partner.

7.3. Transport control

Information that is sent by email is protected with server-to-server encryption.

SIM cards, flash drives, USB sticks and other removable data media must be controlled and stored safely outside of Qualibroker AG. Removable data media must be encrypted if this is technically possible.

Documents to be shredded by the outsourcing partner are stored and transported in sealed containers until the time of their actual destruction.

7.4. Disclosure control

In accordance with Art. 9 para. 1(d) DPO, it must be possible to identify the recipients of personal data disclosed via data transfer equipment. Sensitive customer data may only be passed on in encrypted form. Data transfers are logged. It is always necessary to check whether the person making the request is authorised to receive the information.

Authorised persons are recorded in the broker software. This information is reviewed by the customer each year during the annual meeting.

7.5. Storage control

Unauthorised entries, changes or deletions on the storage are prevented using access and authorisation control (e.g. user name/password) and IT applications. Operating systems and applications are updated regularly in order to minimise the risk of malware attacks.

Copies of all digital documents are created twice a day to protect sensitive data from loss. These copies are deleted after one week. Back-ups are performed weekly, monthly and annually by the outsourcing partner responsible for IT. The annual back-ups are retained for the entire term of the contract. Qualibroker AG stores an annual back-up in tape format in the company safe. Qualibroker AG receives this tape from the outsourcing partner.

7.6. Authorisation control

The Qualibroker AG information system can only be accessed with the relevant authentication credentials. Individual user names and passwords are set for every employee. Employees receive these from the IT coordinator, who also manages this data, on their first day of work. The IT coordinator resets all password every year. It is not permitted for the same password to be reused for the same user. The IT coordinator only allows strong passwords to be used. If login credentials are entered incorrectly multiple times, access to the information system is blocked and must be reactivated manually by the IT coordinator.

A firewall protects the system against use by unauthorised persons outside of Qualibroker AG. IT security measures are in place to ensure that security is continuously monitored.

7.7. Input control

Unauthorised storage inputs must be prevented and it must be possible to review in the systems when and by whom all personal data was entered. All entries and modifications must therefore be monitored and logged for security and data integrity reasons.

7.8. End device measures

On their first working day, all employees receive an individual password for computer access. This password must be treated as highly confidential and must not be shared with third parties. The use of all software and the entire operating system of Qualibroker AG outside of the IT resources owned by Qualibroker AG is permitted only with the express approval of Qualibroker AG. Employees are required to use access control to protect the device when leaving the workplace.

7.9. Separation of test and production servers

In order to test new software components, data is copied to a test server. All tests are conducted on the test server and only use the data on the test server.

7.10. Data breaches

Any data breaches that are identified must be reported to the relevant line manager and internal data protection officer immediately. The reporting obligation pursuant to Art. 22 draft D-FADP is then fulfilled. A corresponding process diagram has been created for internal use.

All data security breaches are recorded in a directory. The following information is recorded:

- Date and/or discovery of the incident
- Who reported the incident
- What happened
- Whether Qualibroker AG is affected as the controller or as the processor
- Assessment of the risk to the privacy and fundamental rights of the data subject(s) affected by the data breach
- To whom notification of the incident was given and the name and date of the notification document
- Causes and effects of the incident
- Which data has been restored – of this, which was restored manually
- How and by whom it was restored
- The measures taken
- Responsible person

8. Rights of data subjects

A natural person who can be identified from the personal data processed by Qualibroker AG is a data subject. Qualibroker AG processes personal data both as a processor of customer data and as the controller for the processing of partner, employee and supplier data. In the first case, the customer is the controller. The data subject rights listed here need to be conferred by the respective controller.

8.1. Duty to provide information on the collection of personal data

In accordance with Art. 14 FADP, Qualibroker AG is obliged to inform data subjects of the collection of personal data where Qualibroker AG is the controller of the data processing.

8.2. Right to information

Any person may request from the data controller information on whether data concerning them is processed, where this data came from, the purposes for which it is processed, to whom the data has been disclosed, the categories of data processed, and the duration of data storage.

The request for information may be made in writing to the data controller's contact address, enclosing a copy of the data subject's ID card or passport.

8.3. Right to access and correction

Data subjects have the right to view the personal data concerning them processed by the data controller. If, despite our efforts to ensure that data is accurate and up to date, incorrect information is stored about data subjects, we will correct this information on request. The data subjects will be informed of the correction once it has been completed.

8.4. Right to deletion

If the applicable laws and regulations do not obligate or entitle the controller to store some of the personal data, data subjects have the right to the deletion of their data from the controller's system.

8.5. Right to data portability

Data subjects have the right to receive the personal data concerning them, which they have provided to a controller, and to transmit this data to another controller without hindrance from the controller to which the personal data has been provided.

8.6. Right to object

If it is not necessary to process data in order to fulfil the contract or, according to the applicable laws and regulations, the controller is not obligated or entitled to process the data, data subjects may object to future processing at any time.

8.7. Right to make a complaint

Data subjects are entitled to lodge a complaint with the responsible data protection authority if their rights are infringed.

9. Final provisions

9.1. Changes to the regulations

The data processing regulations are updated on a regular basis. These regulations are subject to change at any time. Changes must be made in writing and require the consent of the Chair of the Executive Board and the data protection officer.

9.2. Approval

These data processing regulations have been approved by the Executive Board of Qualibroker AG and enter into force on 21 June 2019.

Urs Thalmann
Managing Director

Daniel Oberhänsli
Member of the Executive Board