quantum leben

Data Protection Policy

V 1.2

Document properties

Document name	Privacy Policy/Data Protection Policy DSGVO_GDPR engl
Version	V 1.2
Entry into force	30.09.2018
Author, Authors	Francine Ringhofer, Erhard Christelbauer
Contact person	Thorsten Klamp
File name	Data Protection Policy DSGVO_GDPR engl

History

Version	Date	Changes	Author, Authors
Draft v 1.0	10.07.2018	Draft	Francine Ringhofer
Finale v 1.0	01.10.2018	Release	Martin Kampik (CEO)
V 1.1	03.01.2022	Release/DPO change and minor changes	Francine Ringhofer/ Thorsten Klamp
V 1.2	10.04.2024	New edition	Thorsten Klamp

Content

1 Subject matter and objectives

This Data Protection Policy regulates the handling and protection of data of natural persons and their processing within Quantum Leben AG (QL) as well as by directly affiliated and contractually bound natural or legal persons. The policy serves to specify and concretize the requirements of the regulation at European level, the General Data Protection Regulation (EU GDPR).

2 Material scope of application

This policy applies to the manual and fully or partially automated processing of personal data within QL that is stored in a file system or physically processed or held in a systematic collection. The regulations therefore apply to both automated processing and manual processing of personal data. Examples of such processing activities may include

- the processing of applicant data for the purpose of filling vacancies
- the processing of employee data for personnel administration purposes
- the processing of customer data for the preparation of offers, contracts and support
- the processing of customer data and data of involved persons for claims settlement
- the processing of customer data and data of persons involved in order to comply with the duty of care and other legal obligations
- the processing of personal data of contractually bound insurance brokers for the coordination of the sales network.

Excluded from the scope of this directive are

- Unstructured file collections and personal paper notes
- Data processed by natural persons (employees) exclusively for personal or family purposes, such as private birthday lists
- Data of deceased persons, unless otherwise regulated by national law
- Anonymized personal data
- Data from legal entities, i.e. from companies themselves.

3 Spatial scope of application

This Policy applies to QL and directly affiliated natural or legal persons and to personal data processing activities carried out by them.

4 Basics

Personal data within the meaning of this policy means: any information relating to an identifiable or identified natural person. This includes, for example

- Employee data: Name, contact (address, telephone number, e-mail address, etc.), date of birth, tax number, employee abbreviation, employee photo, login data, expense reports, cell phone bills, etc.
- Customer data: Name, contact (address, telephone number, e-mail address, etc.), customer number, login data, health data, tax number, assets, information on family environment, etc.

Anonymized data is therefore not personal data.

Special categories of data: These are particularly sensitive data such as: health data, criminal records, debt collection excerpts, religious beliefs, sexual orientation, children's data, etc.

Processing includes: The inspection, collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure and destruction of personal data.

Responsibility for processing: QL is responsible for the data protectioncompliant requirements for the processing of personal data. The implementation of and compliance with the data protection requirements is the responsibility of the employees and the directly affiliated natural or legal persons.

5 Principles for the processing of personal data

The principles are:

Legality, good faith, transparency

- Earmarking
- Data minimization
- Correctness
- Memory limitation
- Integrity and confidentiality.

5.1 Lawfulness of data processing

Those responsible for the data processing process document the lawfulness of each processing of personal data. The documentation takes place in the register of processing activities, which is kept centrally (link to the processing register).
As an example, and without any claim to general validity or completeness, the most common legal bases are explained below for better understanding:

Firstly, on the basis of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

> *Example: Application for insurance benefits by end customers via our insurance brokers, processing of payments within QL on the basis of broker agreements and order processing contracts.*

Secondly: to fulfill legal obligations

> *Example: Compliance data to fulfill due diligence obligations, data for international tax information exchange AEOI and Fatca, reporting of social security data to the authorities and social security partners, processing of personal data to fulfill statutory retention periods.*

Thirdly: For the purposes of the legitimate interests pursued by QL or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

> *Example: Disclosure of personal data to contract data processors for outsourced actuarial activities and for administration and support purposes, disclosure of personal data to reinsurers, to ensure the availability, authenticity, completeness and confidentiality of stored or transmitted personal data and for the security of related services, or where processing is necessary for the establishment, exercise or defense of legal claims.*

Fourthly, if there is no legal basis for the legal bases listed above, the data subject must give their consent. The processing of special categories of data always requires explicit consent.

> *Example: Noting and saving personal data that is not necessary for the creation of a policy, such as wedding date, personal interests, etc.*

> *Example: Saving and using photos of employees for marketing purposes, on the website, etc.*

Example: The existence of explicit and written consent for the evaluation of health data (e.g. information on existing physical complaints, medical history, medical reports, etc.).

If there is no legal basis for the processing, the processing is unlawful and the personal data may not be processed.

5.2 Good faith, transparency

In addition to lawful processing, any processing must also be carried out fairly and transparently. There must therefore be transparency for the data subjects as to whether their data is being processed, for what purpose and to what extent. Transparency requires that QL fulfills its duty to inform the data subjects.

5.3 Purpose limitation & data minimization

Purpose limitation is a central principle. The defined purpose determines which data is required and may be processed for this defined purpose. It is also possible to have several purposes at the same time.

Example: Collecting data from customers for the purpose of drawing up contracts, legally required compliance checks and for the purpose of fulfilling the statutory retention period for business documents.

It is therefore generally not permitted to process the collected and processed data for another purpose without justification.

This also includes the principle of data minimization; namely, only data that is actually needed to fulfil the purpose and for which there is legitimacy may be collected and processed. Data must be used sparingly, both in terms of the amount of data and access to this data.

Example: Our insurance brokers make sure that no personal data is recorded in their applications for which there is no legal basis, e.g. wedding date, personal interests.

5.4 Correctness

If personal data is processed, it must be factually correct with regard to the purpose of processing. Corrections reported by customers or insurance brokers are promptly adjusted in the administration system and existing documents.

5.5 Memory limitation

The storage limitation describes a time limit for processing. QL stops processing the personal data after this time limit has expired, for example by deleting or anonymizing this data.

> *Example: Centrally managed personal data of customers is deleted or anonymized by QL after a certain period following the termination of a business relationship. The personal data managed decentrally by insurance brokers must also be deleted by them if they are no longer required.*

5.6 Integrity and confidentiality

The processing must ensure the appropriate security of personal data. To this end, suitable technical and organizational measures must be taken to ensure integrity and confidentiality. Further information in this regard can be found in the chapter "Security of processing".

6 Internal data protection organization and responsibilities

6.1 Responsibility for the principles of processing

The management is responsible for the specification of and compliance with data protection regulations within QL.

The delegation of tasks to other persons does not release the management from overall responsibility, but merely allows the actual implementation of the requirements within the QL at operational level.

6.2 Responsibility for the processing activity

In accordance with the previous section (point 6.1), the management delegates the implementation of the requirements of this guideline to each owner of a processing activity (process owner, specialist manager). They are responsible for ensuring compliance with data protection requirements in their own area and are obliged to provide the necessary information to the data protection officer, to disclose it to him and to provide support in monitoring compliance with internal data protection requirements and the GDPR or legal obligations.

This responsibility is documented and filed in the register of processing activities.

6.3 Data Protection Officer

6.3.1 Organization

QL appoints a data protection officer.

The Data Protection Officer is an employee of QL and is appointed on the basis of his or her professional qualifications and expertise in the field of data protection law and practice.
QL shall provide the data protection officer with the necessary resources and access to personal data and processing operations in his area of responsibility in order to fulfill the respective tasks.

The Data Protection Officer is independent in his duties and consultations and reports directly to the highest management level.

6.3.2 Contact us

The Data Protection Officer is able to communicate effectively with those affected by the provisions of the data protection regulations and to cooperate effectively with the supervisory authorities.

The person of the data protection officer, contact options and communication channels with the data protection officer are communicated by QL in a way that is easy to find for all employees (link). QL also announces the appointment of a data protection officer on its website and provides the email address of the data protection officer dataprotection@quantumleben.com for contact purposes.

6.3.3 Tasks of the data protection officer

The Data Protection Officer performs his duties in an advisory capacity.

Specifically, the Data Protection Officer performs the following tasks, although this list is not exhaustive:

Consulting and monitoring:

- To apply risk management to assess the risks associated with existing processing activities for data subjects
- To carry out a data protection check in advance of a processing activity (privacy by design and privacy by default)
- To provide template documents for data processing partners, for example
- To check suitable technical and organizational measures for the security of the processing of the IT infrastructure
- To carry out data protection impact assessments and prior consultation of the supervisory authorities, where applicable

- To check the transfer and provisions of the bases for data transfers to third countries or international organizations
- To inform QL, processors and employees about compliance with this Directive and the Regulation
- To raise awareness and train employees involved in the processing operations
- To keep a record of processing activities based on the declarations and notifications of the process owners responsible for the processing.

To this end, the DPO is responsible for directives, templates and processes in connection with the GDPR and makes these available at (link).

As part of regular audits, the data protection officer is authorized in particular to

- Collect the information to identify data processing activities
- Analyze and monitor compliance with the requirements for data processing activities
- Inform and to advise the responsible persons and submit recommendations to them.

The data protection officer also provides support with the following tasks:

- Reporting personal data breaches to the supervisory authorities in the role of QL contact person for the supervisory authorities
- Coordinating the notification of data subjects affected by a personal data breach

If the controller does not comply with the recommendations of the data protection officer or does not agree with them, this must be justified and documented by the data protection officer.

7 Obligations for the processing operations

7.1 Data protection risk management

The QL assesses the data protection risks of the processing activities. The risks assessed in this way are in addition to the principles of processing:

- Correctness
- Non-linkability (profiling)
- Intervenability (rights of the data subjects)

- Availability
- Confidentiality
- Integrity

The results of the risk assessment are documented in the processing register. If processing is likely to result in a high risk to the rights and freedoms of natural persons, the data protection officer shall, together with **the process owner,** carry out a data protection impact assessment in advance and identify suitable technical and organizational measures to reduce the risk. If this does not lead to a significant reduction of the risk, the data protection officer consults the competent supervisory authority in advance.

7.2 Privacy by design & privacy by default

When redesigning, adapting or canceling a basis for a processing activity, such as updating an application, involving a processor or expanding the personal data to be processed, the data protection officer must be involved at an early stage during the planning phase to ensure data protection-friendly default settings (privacy by default) and data protection-friendly technology design (privacy by design).

This concerns, for example

- The change of data types and categories, also by reissuing a checklist
- Changes to legal bases and obligations
- The creation of new and regular evaluations
- The change to systems with which data is processed
- The involvement orthe change of a commissioned data processing relationship (supplier)

A processing activity may not be implemented or mutated without a review by the data protection officer and, if necessary, the implementation of the recommended technical and organizational measures. The data protection officer documents the results of the risk assessment and any technical and organizational measures and updates the record of processing activities as required.

The process description and the procedure are:

a) Technical changes: All adjustments to applications, websites, portals, etc. are controlled centrally. If there is a need for changes or adjustments, these must be reported to the data protection officer. This does not apply to regular updates or maintenance work on IT systems or applications that have no influence on the basic processing procedures, such as updates to operating systems, standard updates in the policy management system, new notebook purchases, etc.

b) New suppliers and partners: If new suppliers and partners are to be brought in who are acting on behalf of and on the instructions of QL, QL's contract template must generally be used and the new partner must be reported to the data protection officer.

Example: Actuarial services, external IT service providers, software manufacturers and operators, etc.
Thereof excluded are: Postal service providers, product suppliers (without data access), telephone providers

c) Changes to the content of processes: Use of data for other purposes or changes in responsibilities.

Example: Transfer of customer master data to new co-insurers or sales partners

d) Each further material change in connection with personal data.

7.3 List of processing activities

With the support of those responsible for processing activities and local contact persons, the Data Protection Officer maintains a central register of processing activities relevant to data protection in accordance with the content requirements of the General Data Protection Regulation.

This processing directory is reviewed regularly on an annual basis and/or whenever there is a change in processing activity. The processing directory is centrally available internally (link to the processing directory).

7.4 Safety of processing

Risk management for the security of processing is carried out by the Chief Risk Officer in cooperation with QL's IT service provider. The Data Protection Officer assesses the results of risk management from the perspective of data protection objectives.

7.5 Data transfers to third countries or international organizations

We do not transfer any personal data to third countries (outside the EU/EEA) without an adequate level of data protection (adequacy decision or Privacy Shield). The transfer of data to Switzerland as a third country is permitted. As part of the Privacy by Design process, the data protection officer checks the data transfer.

Examples of such a transfer are the use of plug-ins on the website, the use of cloud services in third countries.

8 Rights of the data subjects

Individuals have the right to be informed about the processing of their data, to obtain information, to object to the processing, to have the data rectified, to request erasure and to restrict the processing or to have the data transferred to another controller.

8.1 The right to information

The controller of the processing activity is obliged to inform the data subjects transparently about the processing when collecting the data.

QL informs the groups of persons as follows:

a) Employees: Information on the processing of employees' personal data is published under the following link. This information or this link is sent to new employees at the latest when they take up their position.
b) Insurance intermediaries: Information on the processing of personal data is published on the QL website under the link http://www.quantumleben.com/de/datenschutz.html
c) Visitors to the websites: Data protection notice on the QL website http://www.quantumleben.com/de/datenschutz.html and on all other websites also under "Data protection"
d) End customers: Information on the processing of personal data is published on the QL website under the link http://www.quantumleben.com/de/datenschutz.html.
e) Other groups of persons: Will be informed individually by the data protection officer

This information can be accessed by the data subjects or their representatives at any time.

8.2 Further rights of the data subjects

In principle, it should be noted that the data protection officer must always be consulted when safeguarding the rights of data subjects, for example when notifying other recipients of personal data.

Example: An end customer would like to know what data is processed by the insurance intermediary as part of their customer relationship. The insurance intermediary contacts the QL data protection officer with this request, who complies with this request for information together with the intermediary's support.

The data protection officer must be informed and involved in every data protection request via the known e-mail address (dataprotection@quantumleben.com). The only exception is the right to rectification if a person wishes to correct data that is actually incorrect. The data protection officer decides on the type and implementation of the response in individual cases.