eb-Qual Privacy Policy Dated January 2022

1 PREAMBLE

Protecting privacy including personal data is very important to us, including ensuring adequate protection of personal data we receive. The present document describes our policies with regards to personal data we receive, why, and how we process it. This Privacy Policies applies and are an integral part of our contracts.

2 ACTING AS DATA CONTROLLER FOR CONTRACT EXECUTION

The personal data typically involved constitutes 'business information'. It relates to identified or identifiable persons, such as name, phone number, address, email, and function within organization. It may also include technical information, i.e., the IP address involved, as well as bank coordinates for payment purposes.

To meet contract performance obligations and ensure that services meet high quality standards, we collect, store, and process, only to the extent necessary, personal data of our clients and providers, to manage commercial relationships, process purchase orders and contracts, provide product and services, bill, and support services. Our data processing includes security and technical operations measures, including some infrastructure, communication, quality, or similar services. Such is the sole purpose of our processing activities with regards to personal data.

Personal data handling may also include that which is necessary to handle analytics and statistics as related to its contractual obligations, for the quality, security and reporting as well as billing activities.

3 ACTING AS DATA PROCESSOR FOR OUR CLIENTS

When managed or cloud services are involved, we handle Client data as a data processor of certain Client data (including Client's content). Client is the appointed data controller (including all related obligations), and we process data exclusively in accordance with the stated contract.

Each party's performance shall comply with Swiss data protection laws, and also, when applicable, standards of EU GDPR directives (General Data Protection Regulation 2016/679). We shall reasonably cooperate with Client in its fulfilment of any legal requirement, such as providing access to personal data, or compliance inspection and audit requests, or when a transfer abroad necessitates additional agreements to protect personal data.

Content data that Clients entrust us by using services, is neither read, modified nor evaluated by us unless required for the sake of the services. Technical and organizational security measures are in place to protect it from unlawful access by third parties. We have no influence over the security of Client content data when it is transferred via public networks. Whenever technically feasible and upon Client's request, specific security measures could be added to the usual services, such as data encryption. Such are at Client's choice and necessitate prior agreement by both parties. Following expiry or termination of services, we destroy Client's content data no later than 90 days (or the time provide by the third party involved), and upon due time Client requests it we can return the content.

We only disclose Clients' data to public authorities when we are legally obligated to do so.

4 TOWARDS THIRD PARTIES

When a third party is involved with the performance of services, we may need to provide Client data. In such case:

- Third parties, may be granted limited and controlled access to the personal data required for business processes, for example debt collection purposes or maintaining IT operations,
- We only disclose as much information as is necessary for services to be provided,
- We will inform you when we use a new subcontractor who has access to personal data.

We furthermore require third parties to deal with data protection in accordance and compliance to the applicable law. Some software vendors may have their own arrangements that overrule our Privacy Policy, such arrangements are to be found in the terms and conditions that apply (and prevail) over our General Terms & Conditions and the present Privacy Policy.