# Documentation of the technical and organizational measures for data protection compliance

Actionbound GmbH, henceforth called “Actionbound”

## Physical Access Control

*Prevent unauthorized persons from gaining access to the data processing systems.*

Regarding the premises where data is processed, it is necessary to distinguish between the data centers and the corporate office.

**Data Centers**

The data centers are operated by Hetzner Online GmbH, 1&1 Internet SE and Amazon Webservices, Inc.. Amazon Web Services is contractually obligated to process all data at the data processing centering in the Frankfurt am Main metropolitan area. The data center operators each have an agreement for order data processing.
Access to the data centers is secured by the operators of the data centers. The normal, high standards of access control for industrial data processing have been contractually guaranteed and was considered when service providers were selected. Documentation can be provided by Actionbound as requested.

**Corporate Office**

The corporate office are the rooms used as the Berlin office and Hohenpeißenberg headquarters of Actionbound. Individual associates who have proven themselves to be especially trustworthy are also permitted to work from other locations (e.g. while on a business trip). Associates in managerial positions, who have proven to be especially reliable, have also been permitted to work in a lockable home office on a case-by-case basis. All employees are obliged in writing to maintain confidentiality and to comply with the data protection requirements under the General Data Protection Regulation. It has been ensured through a directive to all associates that the corporate office may not contain any unencrypted organizational or customer data, nor may any organizational or customer data be taken out of the corporate office.

For this reason, there is also no requirement for special access control at the corporate offices. The security measures employed are standard for commercial spaces, e.g. a locked door with a key registry and security shutters.

## Logical Access Control

*Prevent unauthorized persons from using data processing systems.*

**Data Centers**

The servers in the data center store both organizational and customer data centrally. Access control to these servers is therefore of particular importance.

The servers in the data centers can be administered with corresponding user accounts. The administration of the servers takes place via the internet, using an encrypted protocol with access via 4096 bit RSA keys. These keys are known only to the management and are changed regularly.

**Associates' Computers**

Access to associates' computers is controlled via user accounts. Every associate has an individual user account both for their local computer and for  the administrative software, with which controlled access to user and organizational data is possible in a customer support context (see data access control). Employees are obliged to use passwords as recommended by the Federal Office for Information Security. The transmission between the data centers to the employees' computers is encrypted.

## Data Access Control

*Ensure that only authorized persons can access data, and that the data may not be read, changed, copied, or deleted without authorization.*

Access to customer data is only possible for trained associates in the sales, accounting, and support departments, as well as for the management.  This is ensured by the special allocation of authorizations by the management to the employees.

Actionbound has a written agreement with each associate that ensures that data will not be read, copied, changed, or removed without authorization.

## Data Transfer Control

*Ensure that data cannot be read, copied, changed, or deleted in the process of transmission/ transport.*

Actionbound ensures data transfer control through the storage location of customer and organizational data in data centers, as well as through restrictions on access to this storage location. Unauthorized reading, copying, changing, or deleting of data saved in the data center by the operators of the data center is contractually excluded. For the purposes of transmission data are encrypted, as is discussed above, under Data Access Control.

## Data Entry Control

*Ensure that it is possible to retrospectively determine whether data was changed or deleted, as well as who changed or deleted it.*

To ensure the data entry control, associates’ actions in the customer administration is protocolled. The data from this protocol can be used at any time to determine which associate undertook each entry or change. Duplicates of the log file are backed up geo-redundantly.

## Control of Processing Instructions

*Ensure that data that are processed on contract  can only be processed in accordance with the instructions of the contractee*

A written contract with all data processors ensures that order data processing occurs only in accordance with Actionbounds’ instructions. Use or transfer of the data by associates of the data processing center is contractually excluded.

## Availability Control

*Ensure that data are protected from accidental destruction or loss.*

The availability of data is ensured using a multi-layered security concept.  The first layer is the server itself, which is equipped with mirroring hard-drives (RAID). There is therefore no data loss when one hard drive fails.  Defective hard drives can be exchanged without disrupting service using a so-called “Hot-Plug” system. The status of the RAID system is observed regularly and the operators of the data center are commissioned with the replacement of a hard drive in the case of a disruption.

The second layer is that the data are also held on a second server at the data processing center, so that access is ensured in the case of disruption of the primary server.

As a third security level, the data is compressed daily and encrypted according to the established state of the art and transferred to a separate, spatially separate backup data center.

The data center offers fully airconditioned security rooms that offer protection from gas, water, and fire. The additional storage location in a back-up data center ensures that data will not be compromised  even in the event of  the most significant accidents that might be anticipated, e.g. the crash of an airplane into the first data center.

## Separation Control

*Ensure that  data stored  for different purposes are processed separately.*

Data that are stored for different purposes (e.g. licenses, Bound creations, Bound results) are saved in different data bases . The test, quality assurance and production systems run on different instances with completely completely separate databases. The databases are logically separated from the application layer. The synchronization of the databases is ensured by replication.

*As of December 1st, 2019.*