Order processing (Technical-organizational measures)

Preamble
In this document, we describe the key technical and organizational security measures we take to protect privacy.
This document is for anyone who is responsible for execution and control. Art. 32 para. 1 lit. b DS-GVO and Art. 25 para. 1 DS-GVO were determined by the client.

Definitions
APP
This is understood to mean the application provided as SaaS.

CLOUD
By this we mean the system engineering environment for the APP. This consists of a STRATO hosted virtual server. Technical and organizational measures of STRATO for data protection are described in detail in point 3.

KD cable Germany

AN The Contractor

AG The client

RAS
Remote Access Room. Local administration room at the AN, access keyed and coded. Access only for authorized employees. Video surveillance active.

SAFE
Data vault at the AN. Fire water protection gem. EN 1047-1 S90. Key and code secured.

sadmin
Administrator Software Solutions Simple

SPK
Bank Safe. Access by named persons in the access list of the bank and keys.

STRATO
SaaS provider (provision of the server platform)

Important NOTE

This document is automatically translated. Binding document for contract german version.

Order processing (Technical-organizational measures)

1. Platform as a Service Provider

The AG has given its approval that the contractor appoints the following subcontractor

Name / Company / Postal address / Country	STRATO AG Pascalstraße 10 10587 Berlin
Services used:	The AN takes from STRATO infrastructure and Platform services, eg. B. computing capacity and storage space to provide the AG the use of the APP as a "Software as a Service" service available. Among other things, the contractor uses the following STRATO services: Virtual Server Windows, Managed Backup, SSL Certificate.
Contractual basics / Further information:	The use of the Strato services is carried out by the contractor within the framework of the general terms of use and security measures of STRATO (available at https://www.strato.de/sicherheit/)
Order processing contract	The Contractor has concluded a contract with STRATO on 09.05.2018 pursuant to Art. 28 para. 3 DSGVO.
Location of servers	The order data stored at STRATO are stored exclusively on servers in Germany .

2. Confidentiality (Art. 32 Abs. 1 lit. b DS-GVO)

2.1. Entry control

System-technical access to the CLOUD is only possible by the AN in the RAS.
Access can only be made from a fixed IP assigned by KD.
The implementation is done by software using appropriate firewall rules.
Access is exclusively via protocols with encryption (secure rdp, secure ftp)

2.2. Access control

All IT systems that are necessary for order fulfillment are password protected. The systems are protected by firewall as well as user name and password against unauthorized access. Workstations / notebooks used for system maintenance and system support have their own accounts

The security level of the passwords is regulated by an internal guideline. The client has no system-technical access to the CLOUD, but only access to the APP in accordance with the agreements.

The AN has assigned the APP a unique domain. Only people registered within this domain can access the APP.

The APP has the system-specific access rights

SADMIN	Manager, full Rights Benannte Person auf Seiten **AN**
ADMIN	Editor, Register new users, Read/Change all documents group
HR	Editor, Read/Change all documents group, can be modified by ADMIN
FIBU	Editor, Read/Change all documents group, can be modified by ADMIN
ALL	Autor, Read/Change/Delete personal documents group, can be modified by ADMIN

The system-technical access authorizations are restricted on the software side by the APP, e.g. Changing documents is only possible in a certain status and is logged accordingly. The same applies to the deletion of data, which are always transferred to a system dumpster before being deleted.

Direct access to the rights management of the APP is only possible on the part of the AN.

The allocation of the group ADMIN is only possible on the part of the AN, the AG gives the AN a corresponding application for membership. The groups HR and FIBU can be modified by all members of the group ADMIN.

If a new person is to join the APP, a member of the ADMIN group can send them an invitation. The invitation validity is factory-set 24h and can be shortened or extended by a member of the group ADMIN.

The invitation contains a link to the APP and a password which has to be changed after the first login. The password quality must meet the security requirements of ISO 27001.

The connection is provided via secure https encryption with a corresponding valid certificate.

After a maximum of 5 unsuccessful login attempts, a user account is locked and must be manually unlocked by a member of the ADMIN group.

With the departure of a user is automatically a deactivation of his access.

2.3. APP Control

The APP can only be reached by the AG via SSL-secured connections.

The APP is equipped with a differentiated access concept. A distinction is made between authorization via roles, groups and persons registered by name.

Each authorized user of the APP is assigned to the authorization group ALL, which allows to open the APP, to create documents and to read documents that have been created, or to change them in certain states. The ADMIN can grant delete rights via the configuration. Further rights are not given for standard users.

Exceptions apply to HR supervisors, deputies and staff units. These are recorded by the AG in a separate organizational database and receive reading rights for all persons assigned to you.

Special rules also apply to the HR and GL groups. These have extended rights to documents and are available for special tasks such as Personnel processing (product allocation, remaining vacation, annual transfer, etc.) is responsible. The assignment of persons to this group is the responsibility of the AG.

As part of the workflow, temporary author rights are assigned to designated persons (for example, decision-makers in the case of a leave request), which are revoked again after the work step has been carried out.

If deletions are made in the APP, the APP transfers them to a separate database before removal, to which only the AN has access. The deletion date and the executing user are logged. The deleted data are held for a period of time that can be set by the PLC and then destroyed.

Changes to documents in the APP are identified by history history, which is carried throughout the life of the document. The logging is done for actions as well as document content changes as well as the changing person.

2.4. Separation Control

There is one virtual domain per client (= domain). This includes all objects of this client such as persons, registrations, absences, etc.)

The APP is operated in its own virtual domain in the CLOUD. Access to the APP is always personal by entering a user name.

This user name is automatically linked to the unique domain name when it was registered, which was assigned to the AG by the contractor when placing the order.

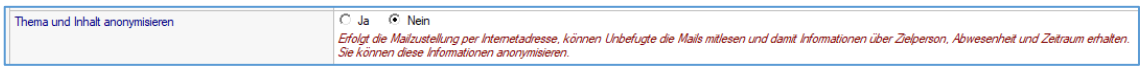
Per APP, a maximum of one domain is possible, cross-domain access is not possible.

3. Integrity (Art. 32 Abs. 1 lit. b DS-GVO)

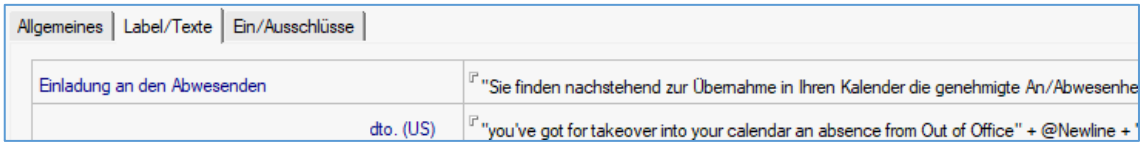
3.1. Transfer Control

As part of the process, the app sends emails that contain information about tasks to be performed. This mail is sent unencrypted and usually contains no relevant personal content.

The AG can completely anonymize this mailing.



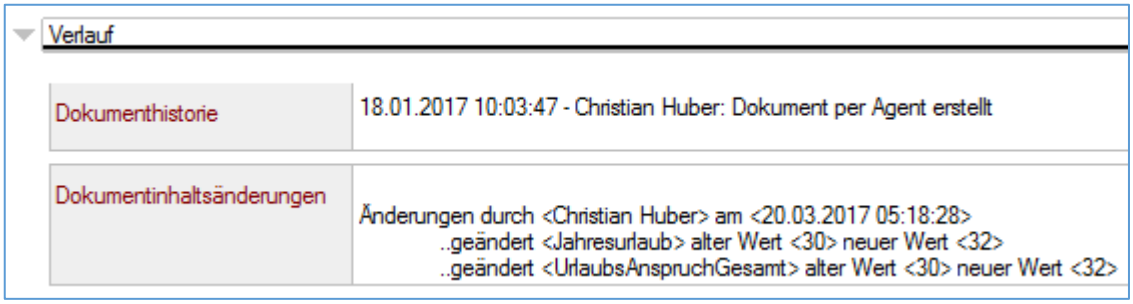
The app can send invitations with time and away information as part of third-party calendar synchronization (e.g., Outlook, Lotus Notes). The shipment is unencrypted. The client can switch the synchronization on / off and completely anonymize texts.



The AN implements a local replica of the APP in the RAS as part of the provision of the APP for data backup, the data are transported over a 256-bit encrypted line and stored at the AN in a permanently installed safe of resistance class S90. The local storage is encrypted, a decryption can only be done by the SADMIN.

3.2. Input/Edit Control

Changes to documents in the APP are identified by history history, which is carried throughout the life of the document. The logging is done for actions as well as document content changes as well as the changing person.



4. Availability and Load-bearing capacity (Art. 32 Abs. 1 lit. b DS-GVO)

4.1. Availability control

The AN only manages client systems locally, the availability of the server systems can be found in the contract data processing contract separately with STRATO.

The AN distinguishes between the availability of the data (e.g., accidental deletion of individual documents) and the availability of the APP (e.g., non-expiration due to an operating system error).

The CLOUD is backed up in full mode before each update. Every 2nd backup is overwritten. There is no backup of data of the APP, this is separately regulated (s.u.).

4.2. Fast recovery (Art. 32 Abs. 1 lit. c DS-GVO)

A technical system recovery is carried out after notification by the AG within 24 hours on weekdays.

In terms of the APP the AN distinguishes here 3 variants

default
The APP is replicated once a day in the RAS (encrypted data transmission, encrypted local storage when the AN is on). It will be stored in the SAFE for a period of 30 days, after which the data will be automatically overwritten.

Pro
Data replication analog standard. Additional storage of monthly and annual backups. Offline storage of an encrypted copy in the SPK.

Premium
Analog Pro. Additionally, provision of a clustered server to which the data is replicated in real time. Recovery time in case of complete failure of the APP within 2 hours after notification on working days between 09:00 and 16:00.

5. Procedures for periodic review and evaluation (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

5.1. Privacy friendly defaults

According to the state of the art, data protection measures are already taken into account in the conceptual development of products as well as projects and procedures. the requirements of Art.25 DSGVO Abs. 2.

5.2. Incident-Response-Management

In the event of personal data breaches, an immediate and legal response is ensured (testing, documentation, notification). Forms, guidance and established implementation procedures with designated persons.

5.3. Order processing control

The processing of personal data is carried out only by the APP in accordance with the instructions of the AG. If further processing by the contractor is desired (for example evaluations), this must be explicitly requested by the client in writing.

The coworkers of the AN are committed to the data secrecy / secrecy / confidentiality.

All coworkers of the AG are familiar with the data processing purpose, on confidentiality and discretion gem. Art. 28 para. 3 lit. b DSGVO committed, advised on possible liability consequences and instructed about the data protection requirements and instructed in this regard and monitored for their compliance.

An IT security concept is available both at the contractor and at the AG and is regularly adapted to changed environmental parameters.

Subcontractual relationships are mandated in writing.