General description of the technical and organisational measures pursuant to Article 32 para. 1 of the GDPR for processors (Article 30 para. 2 (d) of the GDPR)

(Status as of: June 2019)

I. Confidentiality (Art. 32 para. 1 (b) of the GDPR)

1. Access control

a. Regulatory content:

Unauthorised persons should be prevented from accessing the data processing, data storage, network and telecommunications equipment used to process data in the order.

b. Technical and organisational measures

All data processed in the order are always stored in secure areas. Access is only possible for authorised personnel.

Visitors have to register at the reception and are always accompanied by an uberall employee. Entry into the work areas is only possible with a security key. The offices are also monitored by security personnel at night, weekends and on public holidays.

2. **Access control**

a. Regulatory content:

The risk of physical, material or immaterial damage or the risk of impaired rights and freedoms for affected persons due to unauthorised disclosure or unauthorised access to the data processed in the order must be reduced. Usage of data processing, data storage, network and telecommunications equipment by unauthorised third parties must be prevented.

b. Technical and organisational measures:

All computers must have an access control system. There must be mandatory rules for password assignment. This concerns the necessary complexity, the lifetime of the password as well as the reuse of old passwords. Media carriers must be encrypted, and the keys must be stored within the server host Amazon Web Services and can only be viewed by authorised uberall staff. Mobile devices of uberall employees must be encrypted. Employees must be regularly briefed and informed in this connection by providing information.

Regarding remote access to the infrastructure there must be no direct connection to servers, and access must run via a central server. Access via password is not possible; access is only via an individual private-key authentication.

To ensure higher protection standards, using of the uberall application requires for the customer to enter a password with minimum length. In addition, the user session is secured by a secure cookie.

3. Access control

a. Regulatory content:

The persons entitled to use IT systems may only access data that is subject to their access authorisation. Data processed in the order must not be read, copied, altered or removed without authorisation during processing.

b. Technical and organisational measures:

The deployed IT systems have a dedicated user rights system, which makes it possible to assign data access and changes based on roles and individual authorisations. There must be mandatory rules for password assignment. This concerns the necessary complexity, the lifetime of the password as well as the reuse of old passwords.

Each employee can only access the necessary data for his activity and the authorisation assigned to him within the scope of his duties.

Anonymous access to internal data is not possible due to the 'Principle of least privilege'. Accesses are always logged centrally and locally.

Each employee's personal responsibility for the security, confidentiality, integrity and availability of data and information is enhanced by centrally-provided information.

4. Separation control

a. Regulatory content

It must be possible for data collected for different purposes to be processed separately.

b. Technical and organisational measures

The principle of functional separation between service and development exists, the integrated departments are functionally and organisationally separated. Data that is worthy of protection is provided to employees only to the extent necessary for the assigned task.

The transition from the development system to the production system is secured by appropriate tools and comprehensibly documented. Data used for development purposes will be anonymised.

5. Pseudonymisation

As a processor, uberall does not take any additional measures for pseudonymisation other than the measures resulting from the respective service descriptions of the services or carried out by the person responsible in the context of the commissioning.

II. Integrity (Art. 32 para. 1 (b) of the GDPR)

1. Distribution control

a. Regulatory content

Data processed in the order may not be read, copied, altered or removed without authorisation during electronic transmission or during transport or storage on data carriers.

b. Technical and organisational measures

For this purpose, state-of-the-art and highly secure encryption methods are used by uberall everywhere for electronic transmission to meet the standards of the requirements.

The electronic transmission of data is encrypted via https and ssl and secured via a VPN connection. Explanations by email are always made with an electronic signature.

2. Data entry control

a. Regulatory content

Changes, entries and removal of personal data must be monitored and logged in order to detect any unauthorised access and to react to it as quickly as possible.

b. Technical and organisational measures

All data input (entry, update and deletion) is saved by the uberall application. Direct data entry into the database is only possible with special rights, which is also limited to a small group of people, and is checked by at least 4 eyes.

III. Availability and resilience (Art. 32 para. 1 (b) of the GDPR)

1. Availability control

a. Regulatory content

Data processed in orders must be protected against accidental or wilful destruction or loss.

b. Technical and organisational measures

Uberall uses Amazon Web Services as a data centre and server host/service provider. Availability of the data is ensured by the following measures:

- The data centre systems are divided into different fire sections.
- Frequent maintenance of the production facilities ensures high availability of the technical equipment.
- Emergency power
- The power supply for the IT systems is redundant and allows the supply of power via dynamic UPS systems (uninterruptible power supply).
- Modern emergency power systems enable the operation of the data centre without connection to the public power grid.
- Fire protection: Early fire detection system; the ambient and outdoor air is set up to detect fire/smoke aerosols.
- Fire sections with fire-retardant walls
- Oxygen-reducing fire extinguishing system
- Sprinkler system
- Air-conditioning: The data centre is air-conditioned via redundant air conditioning systems and spatially separated, redundant refrigeration units, which work in conjunction with each other.

Uberall also ensures optimal availability by making backups several times a day and storing them in different locations (SQL or direct snapshot). In addition, each component is redundant and secured by a firewall.

2. Recoverability

a. Regulatory content

The risk of physical, material or immaterial damage or the risk of infringement of rights and freedoms, including unlawful or negligent acts for affected persons through destruction, loss, modification or unauthorised disclosure of data processed in the order or the unauthorised access to it by a physical or technical incident must be reduced.

b. Technical and organisational measures

Database snapshots can be restored at any time. The infrastructure can be restored within a few hours through highly automated procedures.

IV. Procedures for periodic review, assessment and evaluation (Article 32 para. 1 (d) of the GDPR; Article 25 para. 1 of the GDPR)

1. Data protection management

a. Regulatory content

Procedures must be followed for the periodic review, assessment and evaluation of the effectiveness of the technical and organisational measures to ensure the safety of the processing.

b. Technical and organisational measures

The effectiveness of the measures is constantly checked by the data protection officer.

The data protection officer's information is below:

Philipp Herold (Meindatenschutzbeauftragter.de), email: dataprotection@uberall.com

2. Incident Response Management

a. Regulatory content

If unauthorised access to data is detected, functional management and associated error analysis or correction must be ensured.

b. Technical and organisational measures

Individual measures are defined via SLA with the respective customer and combined with response times for different scenarios. In addition, an internal emergency service is implemented, which is responsible for both the infrastructure and the application.