TOMS

Appendix 1 - Technical and organizational protective measures

(Security of processing in accordance with Article 32 GDPR)

Save as pdf

Preamble

Taking into consideration the state of the art, the cost of implementation and the type, scope, circumstances, and purposes of the processing as well as the varying probability of occurrence and the seriousness of the risk for the rights and freedoms of natural persons, this appendix specifies the technical and organizational protection measures, as referred to in Article 32 of the EU Data Protection Regulation ("GDPR"), arising from the underlying data processing in order to ensure an adequate level of data protection for the risk.

This appendix shall apply to all activities whereby employees of the order processor (Contractor) might come into contact with personal or other data of the Responsible Body (Contracting Authority).

§1 The technical and organisational security measures to ensure an adequate level of data protection

meetyoo conferencing GmbH
Friedrichstraße 153a
10117 Berlin, Germany

(1) Measures to ensure permanent confidentiality:

The relevant operational meetyoo systems are located in a certified and specially designed high-security data centre in Berlin for the operation of IT infrastructure.

meetyoo is certified according to ISO 27001. The current certificate can be found at the following link:
https://www.certipedia.com/quality_marks/9105037096?locale=en

Access control:

Data centre access control system meetyoo:
Access is made to the leased data centre areas via an access chip in combination with a PIN code. The access chips are personal and are specifically assigned to authorised employees by name. In addition, access to the areas must be registered in advance.

Access chips are only issued to trained employees and, like the use of the chips, this is logged. External personnel may only enter the data centre areas under the constant supervision of a meetyoo employee. Both the areas and the access points to the areas are under 24-hour video surveillance. The meetyoo server cabinets are individually lockable.

Friedrichstrasse office space access control system:
Access to the office space in Friedrichstrasse is controlled by an access card system. Issue and use of the cards are logged, and the permitted access times are adapted individually. Visitors and third-party staff are provided admittance by reception personnel and accompanied to the desired contact person.

Public access to the office building is possible on weekdays from 7:00 am - 8.00 pm. Outside of these times, an additional access card is required to unlock the entrance doors and the elevator. This additional card is only issued to selected employees. Both the issue and usage of this is logged. A concierge is always present in the foyer area of the building (24x7).

All doors are manufactured in intrusion-retardant and—insofar as they are emergency exits—secured by a local alarm system. The offices are located on the third floor. The windows can only be tilted downward with a very narrow-angle and are made of safety glass, so that penetration is not possible.

Access control system data centre AWS:
The data processing equipment used for the virtual events is located in the data centre of the company Amazon Web Services EMEA SARL in Frankfurt or Paris. The data centres are certified according to the current standards: ISO 27001, ISO 27017, ISO27018, , SAS 70 Type 1, PCI DSS Level 1, HIPAA.

Physical access to the AWS data centre is strictly controlled by professional security personnel, both at the perimeter and at the building entrances. Video surveillance and state-of-the-art attack detection systems and other electronic equipment are used. Authorised staff must undergo two-factor authentication at least twice before being allowed to enter the data centre floors. All visitors and contractors must identify themselves and register. Visitors will be accompanied by authorised staff at all times.

When authorised people register, they are issued with a badge that requires multi-factor authentication and restricts access to previously authorised areas.

Access to the data centre is logged and regularly audited by AWS staff.

More information on the AWS security concept:
https://aws.amazon.com/de/security/

Access control:
Authorizations are assigned exclusively within the context of the contractual obligations for the provision of the necessary scope of respective work.

Password rules: **Access to systems** of meetyoo is controlled via password. An individual user login when logging on to the system is safeguarded by strict password rules. This includes special characters, minimum length and regular changes of passwords, among other things.

Screen lock: According to the **Use Agreement for IT Workstations**, every employee of meetyoo is obliged to lock his or her screen when leaving the workplace. In addition, the screen is automatically locked after five minutes of inactivity. Workstations of employees, who often have to leave their workstations for a short time due to the nature of their work (e.g., reception), are also secured by a USB dongle.

Access control:
Authorizations are assigned exclusively within the context of the contractual obligations for the provision of the necessary scope of respective work. The authorizations for access to the various systems are granted only after an employee has worked through the respective initial training plan and only after approval by the department head. These approvals are documented centrally. This also applies to the administration area of systems. The administration is also carried out only with personal accounts insofar as possible.

The data concerning authorisation concepts and needs-based access rights and the logging of accesses are protected from unauthorised reading, copying, modification or removal.

The network of meetyoo is divided into several zones separated by firewalls. Strict attention is paid to the design of communication between these zones to ensure that no communication from the demilitarized zones into the internal network from meetyoo is permitted.

Personal data is stored in the internal network as far as possible. The security of these measures is regularly audited by external service providers and internally in the context of a penetration test (as black and white box tests).

Virus protection is carried out in accordance with a defined and documented process. All client computers are equipped with appropriate anti-virus software and communicate regularly with a central server, which ensures that the signatures are current. This central server checks all outgoing e-mails for any possible virus infection to ensure that no viruses are brought into circulation from the network of meetyoo. In addition, all

incoming e-mails are checked for viruses with the help of a service provider. Affected messages are not delivered.

Separation Control:

The network of meetyoo is divided into several zones separated by firewalls. Strict attention is paid to the design of communication between these zones to ensure that no communication from the demilitarized zones into the internal network from meetyoo is permitted.

Personal data will only be collected within the framework that is **absolutely necessary** for our provision of services. Once the data is no longer required, this is **deleted.** The review of a data portfolio for data that is no longer required takes place in accordance with a specified review schedule. This does not affect the individual right to information, rectification and deletion of personal data in accordance with Art. 15 – 17 (GDPR). Information requests can be made to the meetyoo's company data protection officer at any time and will be answered as swiftly as possible. The deletion of itemised bills is additionally subject to the requirements of the TKG (Telecommunications Act). These will, of course, be observed.

Changes to existing systems as well as the introduction of new systems is carried out in principle only after an **extensive test** in a meetyoo test network **completely decoupled from the operating network**. Before porting any such modification/new feature into the operating network, a documented acceptance test and an FMEA are conducted, including the definition of appropriate countermeasures.
The **patching of IT systems** is carried out in the context of the documented patch management process. New patches are first tested in a lab environment and then installed in the operating system. The designated time frames are dependent on the risk class of the errors to be patched.

(2) Measures to ensure integrity on a permanent basis:

Measures to prevent the unauthorised reading, copying, modification or removal of personal data during electronic transmission or transport.

a) Forwarding control
Establishment of dedicated lines or VPN tunnels. Encrypted transfer of data from or to the external networks by means of appropriate transport protocols.

b) Input control
Rights to enter, change and delete data are assigned on the basis of an authorisation concept. The input, modification and deletion of data are not traceable by individual user names (not user groups).

(3) Measures to ensure availability on a permanent basis:

The **relevant operating systems** from meetyoo are redundant.
All business-relevant data from meetyoo are backed up at regular intervals within the context of a structured backup plan. This also applies especially to personal data. The proper execution of backup jobs is checked on a daily basis. An archive is also created once a month. The archived data are stored in a safe. An emergency exercise is also performed once a month, during which the recovery of data from the backup is tested. The result of the test is documented.

There is an **emergency manual**, in which all different error scenarios and appropriate operating procedures for resolving them are documented for all relevant operating systems of meetyoo. This emergency manual is part of our quality and information security management system and is subject to regular review (at least annually). On the basis of this emergency manual, drills are conducted quarterly to check and ensure the correct response for each entity involved.

The business systems of meetyoo are located on a **data center** area designed specifically for the operation of IT infrastructure. The power supply

is provided via two separate supply rings, which are each secured via a UPS. The UPS guarantees a bridging time of 30 (thirty) minutes at a full load. Additional protection is provided out by means of a diesel engine that guarantees power supply for an additional 24 (twenty-four) hours.

There is an **early fire detection** system and a non-toxic, gaseous fire extinguishing system on the data center area.

AWS data centre
In order to protect the account and user data against loss, they are backed up several times a day. The backup of the database is secured by the Amazon S3 service (Cloud Storage Service) with multiple mirroring. Unchangeable data (e.g. videos, log files, etc.) are backed up by the Amazon Glacier service. Both offer a "designed durability" of 99.9999999%. Every three months, a check is made to see if the process of restoring backups is working.

(4) Measures for the use of pseudonyms and anonymisation of personal data:

There is a strict separation of customer master data and customer sales data, through the use of systems that are separate from each other. This involves a CRM and an ERP system. Under compliance with the applicable laws, the data will be anonymised automatically. After the expiry of the respective storage period, this data shall also be deleted automatically.

(5) Measures for the encryption of personal data:

The data exchange of personal data is carried out with the use of the following encryption mechanisms:

-Use of encrypted passwords
-Encrypted transfer of data from or to external networks by means of

appropriate transport protocols (SSL/TLS, etc.)
-Use of encrypted data carriers and mobile devices

(6) Measures to ensure the capacity of the systems and services on a permanent basis:

Within the framework of our information security management system, regular and documented penetration tests are carried out. Devices for monitoring temperature and humidity are installed in the server rooms. The systems and services are designed in such a way that ad hoc instances of high burdening with processing operations are possible.

AWS data centre
As part of information security management, regular and documented penetration tests are carried out in Amazon's data centre. Amazon's systems and services are designed in such a way that even selective high loads of virtual events are possible.

(7) Measures for rapid restoration of availability in the event of a physical or technical incident:

All meetyoo business-relevant data is backed up at regular intervals within the framework of a structured **backup plan**. This applies also and in particular to personal data. The proper execution of the backup jobs is checked on a daily basis. In addition, an archive is created on a monthly basis. The archived data is stored in a safe. An emergency exercise also takes place on a monthly basis, within the framework of which the restoring of data from the backup is tested. The result of the test is documented.

AWS data centre
The account and user data are backed up several times a day as part of a structured backup plan using the Amazon S3 service. Every three months, it

is checked whether the backup process is working.

(8) Measures for regular review, assessment and evaluation of the effectiveness of the technical and organisational measures:

meetyoo is certified according to ISO 27001. The current certificate can be found at the following link: https://www.certipedia.com/quality_marks/9105037096?locale=en

Within the context of our information security management system, the technical and organisational measures for the protection of personal data are regularly audited and evaluated.

All employees are obliged to maintain data secrecy and are given regular training.

A data protection officer has been appointed and works closely with meetyoo to support the implementation and evaluation of our data protection management system.

(9) Measures for data deletion and restriction of the processing:

meetyoo takes the following measures for data deletion:

-Data deletion by means of software including logging
-Physical destruction of the data carriers including logging
-Shredding of paper documents including logging