Technical and organizational measures (TOM) pursuant to Art. 32 I GDPR of Yoummday GmbH, Infanteriestraße 11a, Haus E2, 80797 Munich

As of 2025

Table of contents

I. Principles

II. IT infrastructure

III. Head of IT

IV. Individual measures

1. Confidentiality

1.1. Access control

1.2. Access control

1.3. Access control

1.4. Separation control

1.5. Pseudonymization

1.6. Measures for encrypting data

2. Integrity

2.1. Transfer control

2.2. Input control

3. Availability and resilience

3.1. Availability control

3.2. Rapid recoverability

4. Organizational control

4.1. Organizational control

4.2 Security and risk management

4.3 Certification

4.4 Incident response management

4.5 Privacy-friendly default settings

4.6 Order control

Responsibility of the controller pursuant to Art. 24 EU GDPR.

I. Principles

As the responsible body, appropriate technical and organizational measures have been taken to ensure compliance with the principles of the European General Data Protection Regulation. This ensures and provides evidence that processing is carried out in accordance with the provisions of the EU GDPR.

The following measures serve to ensure the confidentiality of the systems and to

- guarantee the confidentiality of the systems and services
- Ensuring the integrity of the systems and services
- Ensuring the availability of systems and services
- Ensuring the resilience of systems and services
- Restoring the availability of personal data and access to it after a physical or technical incident.
- Procedures for regularly reviewing, assessing, and evaluating the effectiveness of the above measures

The technical and organizational measures to be taken are based on:

- State of the art
- the implementation costs
- The nature, scope, context, and purposes of processing
- the varying likelihood and severity of the risk to the rights and freedoms of natural persons

This ensures a level of protection for personal data that is appropriate to the risk. The measures are regularly reviewed and updated to maintain the level of protection.

II. IT infrastructure

See document: Technical setup

III. Head of IT

Head of IT:

Wolfgang Maier, Head of IT

Email wolfgang.maier@yoummday.com

Deputy:

Florian Neumeier, VP Product & Technology

Email: florian.neumeier@yoummday.com

Data Protection Officer:

Björn Barthelmes
Karl-Frank-Straße
35
12587 Berlin
Email datenschutz@yoummday.com

Data protection coordinator:

Sarah Klein, Legal Privacy Counsel

Email sarah.klein@yoummday.com

IV. Individual measures

1. Confidentiality (Art. 32 (1) (b) GDPR)

1.1 Access control

Protection of rooms containing data processing equipment against unauthorized access

Requirement	Status
Security device Property	(+) The premises where the computers are located are partially fenced in. (+) Gate system with registration
Site surveillance	(+) Video surveillance with camera control, (+) Video surveillance is indicated by signs
Access control system Building security	(+) Locking system Security lock (+) Locking system Digital lock with coded key (+) Locking system: RFID chip
Central reception area	(+) All visitors must register at reception, be entered in the visitor list and accompanied throughout the building.
Access control system for business premises	(+) Locking system: security lock (+) Locking system: RFID chip
Measures to be taken in the event of loss of a key/card/chip	(+) Replacement of the locking system with keys (+) Reprogramming of the code
Building surveillance systems	(+) Smoke alarm system

	(+) Fire alarm system
Securing server rooms	(+) Locking system with digital lock and coded key
External service providers	(+) All external tradespeople, building and data center technicians must register at reception before starting work. Reception will inform the employee expecting the visitor and arrange for them to be collected. If neither the requested employee nor another employee familiar with the task for the external tradesperson, building or data center technician is available, access must not be granted.
Keys/key issuance	(+) Keys are issued by the central building management. (+) Every key issued is recorded in a key logbook or key management system.
Special protection of the data center	(+) Division of the data center according to the shell principle. (+) Access to the data center rooms via airlocks. (+) Video surveillance (+) Motion detectors (+) Smoke detectors (+) Temperature monitoring (+) Alarm system

Data center of Yoummday GmbH:

Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany, Tel.: +49 (0)9831 505-0, Fax: +49 (0)9831 505-3

The full address of the data center is as follows:

Hetzner Online GmbH, Am Datacenter-Park 1, 08223 Falkenstein/Vogtland.

1.2 Access control

Protection of computer systems against unauthorized access

Requirement	Status
Access to systems only via access authorizations	(+) Access to the systems is always granted via a user ID and a correspondingly secure password
User authentication	(+) User ID and password (+) Minimum password length
Password convention check	(+) Approval only by administrator
Rights management	(+) There is a rights concept for rights management. (+) All authorizations are documented in a traceable manner (+) Rights are changed in the following cases (+) Departure of an employee,
Screen lock	(+) Screen lock with password identification is set up for periods of absence.
Firewall	(+) Open source iptables
WLAN	(+) Physical separation of guest WLAN from company network
Notebook security	(+) User ID and password
Logging and monitoring of incorrect logins	(+) Failed logins are logged and evaluated as needed.
Automatic PC lock (e.g., password and break mode)	(+) The PC automatically locks after 10 minutes.

Secure connection for "remote access"	Remote access to systems from your home office using your own PCs and laptops is only possible under the following conditions. (+) User ID and password (+) Data is transmitted in encrypted form

1.3 Access control

Access control measures are designed to prevent unauthorized activities (e.g., unauthorized reading, copying, modification, or removal) in IT systems outside of granted permissions.

A strictly monitored authorization concept with personal user accounts has been set up.
Access to certain information is granted via a group or role concept.
role concept.

Protection of data against unauthorized access

Requirement	**Status**
Written administration concept	(+) Uniform IT security guidelines (+) Separation of responsibilities (+) Administrators are in-house employees (+) Separation of administrator accounts by system and person
Identification and authentication of administrators	(+) User ID and password
Admin password conventions	(+) Minimum character length for alphanumeric characters, (+ exclusion of trivial passwords, (+) Password entry with encrypted process

	(+) Secure password files
Role-based authorization concept	(+) A role-based user authorization concept is in place.
Restrictive rights assignment system	(+) Access authorization is always based on the principle of restrictive rights assignment.
Logging of system usage	(+) System usage is logged via LOG files of the corresponding systems.
Access to data only via access authorizations	(+) Data is accessed using a user ID and a secure password, as well as the assigned access authorizations (roles)
Authorizations only after approval by superiors	(+) Access authorizations (roles) are requested and approved via an electronic workflow
Regulations for the withdrawal of access authorizations	(+) Access permissions (roles) are revoked via an electronic workflow
Authorizations are only granted by authorized persons	(+) Authorizations are only granted by authorized persons using an electronic workflow
Control of authorizations	(+) Authorization assignments are checked regularly
Special authorizations	(+) Special access authorizations are only granted in exceptional cases by a specially authorized supervisor.
Declarations of commitment for administrators	(+) Upon hiring, employees are required to comply with data secrecy, data protection, and telecommunications secrecy, and, where necessary, social secrecy. Awareness training is provided upon hiring and regularly

training sessions for administrators	(+) Administrators receive regular training in information security.
Controlled destruction of data and printouts	(+) The controlled destruction of data and printouts is carried out by specialized, certified service providers

1.4 Separation control

Separation of data sets that are processed for different purposes

Requirement	Status
Purpose limitation of the systems	(+) The systems are managed in accordance with the company's data protection policy based on a strict rights concept.
Rights concept according to data purpose	(+) The rights concept is strictly based on data separation.

1.5 Pseudonymization (Art. 32 (1) (a) GDPR; Art. 25 (1) GDPR)

If pseudonymization is intended for data, personal data is processed in such a way that the data can no longer be attributed to a specific data subject without the use of additional information. This additional information is stored separately and supported by appropriate technical and organizational measures.

The following pseudonymization procedures are used:

- Anonymized identifiers that can only be resolved with the aid of a separate database.

1.6 Measures for encrypting the data

The purpose of measures to encrypt personal data is to protect the contents of databases from unauthorized access and modification.

All personal data and other confidential information is always transmitted in encrypted form. Either a secure HTTPS portal is used for this purpose, or password-protected zip files are sent electronically.

Email encryption is possible on a reciprocal basis. The

following encryption techniques are used:

- TLS encryption for email traffic

2. Integrity (Art. 32 (1) (b) GDPR)

2.1 Control of disclosure

Care is taken to prevent unauthorized reading, copying, modification, or removal during electronic transmission or transport.

Requirement	Status
Organizational specifications for the storage of data carriers	(+) Internal company rules for handling data carriers
Secure rooms for data storage	(+) Data backups are stored either in a secure room (e.g., data protection room, data center) or externally by an appropriate service provider
Data carrier disposal in accordance with data protection regulations	(+) Physical destruction of data carriers is carried out in accordance with DIN 66399, minimum security level 3)
Identification and authentication of participants	(+) Identification and authentication of participants is carried out using user IDs, phone numbers, identification, and passwords. User ID
Encryption of emails	(+) Highly sensitive data is only transmitted in encrypted form

2.2 Input control

Documentation of whether and by whom personal data has been entered, changed, or removed in data processing systems. (Logging, document management)

Proof of data entry or modification

Requirement	Status

Access regulations	(+) Access regulations and user authorizations are in place, enabling the identification of all users and data stations in the system
Logging of the setup and operation of the IT system	(+) Documentation of all authorized users with rights profiles (+) Documentation of the usage rights that have been set up
System logs	(+) User activity is logged in system logs. Input control in database systems is carried out within the framework of the standard procedures supplied with the database systems, which, depending on the database system, may include all entries up to the point of recording. If booking journals are possible in the software systems, these are filled in.
Retention of system logs	(+) System logs are stored in accordance with legal and contractual requirements.
Logging functions	(+) User activities can be tracked using comprehensive logging functions.
Change logging	(+) Changes are logged on the servers or in the programs.
Databases	(+) Input control in database systems is carried out as part of the standard procedures supplied with the database systems, which, depending on the database system, can include the recording of all entries
Table logging	(+) If software-based table logging and an audit information system are available, these functions can be used to perform the relevant checks.

3. Availability and resilience

3.1 Availability control

Protection against accidental or deliberate destruction or loss of data.

Requirement	Status
Regular data backups	(+) Data is secured in backup systems and can be expanded with redundant systems. This ensures a short recovery time and high overall availability in the event of a disaster scenario.
Mirroring of hard disks, e.g., RAID procedure	(+) Data is mirrored regularly (RAID systems, mirroring to physically separate systems).
Uninterruptible power supply (UPS)	(+) The data centers are protected against power failures by separate UPS systems with battery backup.
Separate storage	(+) Data is mirrored regularly (mirroring to physically separate systems). Separate storage of data takes place
Virus protection/firewall	(+) Virus scanners and firewall systems on all systems.
Backup system	(+) System designation: TG2
Contingency plan	(+) The company has an emergency plan and corresponding manuals for maintaining core processes in the event of a crisis. A customer-specific crisis manual is created and maintained on a regular basis.

3.2 Rapid recoverability

Emergency plans/crisis plans/disaster recovery plans exist for the data centers. These are documented in the backup and emergency concept. The functionality of this concept is checked at regular intervals. The emergency plans are subject to a regular review and improvement process.

4. Organizational control

4.1. Organizational control

Organizational measures to ensure the processing of personal/sensitive data

Requirement	Status
IT security concept	(+) An information security guideline is available in its current version and can be viewed on site.
Password policy	(+) The password policy is available in its current version and can be viewed on site.
Data protection policy	(+) A data protection policy is available and can be viewed on site.
Data protection officer	(+) An external data protection officer has been appointed
Employee obligations under Art. 29 +32 GDPR	(+) All employees are bound to data secrecy and compliance with trade and business secrets and are instructed in accordance with GDPR, Articles 29 and 32 (4) to process personal data only on the instructions of the controller.
Employee obligation under TDDDG	(+) Furthermore, they have been bound by Section 3 (2) No. 2 TDDDG.
Subcontractors	(+) Subcontractor guideline is in place.
Training	(+) In mandatory annual training courses, all employees must demonstrate their data protection awareness to their managers. They ensure the binding implementation of the data protection and information security requirements that are mandatory on the company-wide intranet.

4.2 Security and risk management

Services are provided on the basis of an information security management system. This includes, among other things, written guidelines, processes, and manuals for IT/data center operations. They are based on legal regulations and internally proven regulations.

The security procedures used are continuously reviewed.

A risk management system is in place that covers both the operational risks arising from tenders, contracts, and projects. In addition, there is an IT security risk management system that deals with process, service, and location-related risks.

The technical and organizational measures for data protection in accordance with GDPR, Article 32, are regularly reviewed as part of ISO certification. In addition, data protection issues are also taken into account in internal process audits.

4.3 Certification

yoummday:

ISO 9001:2015

ISO 27001:2022 (information security management) Data

center:

ISO 27001:2022 (information security management)

4.4 Incident response management

Security incidents are handled using standard operating procedures and tool-supported processes in order to restore trouble-free operation as quickly as possible. Security incidents are monitored and analyzed in a timely manner. Depending on the type of incident, the relevant and necessary employees from the specialist departments and specialists are called in to deal with it.

4.5 Privacy-friendly default settings

Data protection-friendly default settings ("privacy by design and by default") ensure that data protection is taken into account at the earliest possible stage in order to prevent unlawful processing or misuse of data. Appropriate technical default settings are used to ensure that only personal data that is actually necessary for the specific purpose is collected and processed (need-to-know principle).

In order to achieve the lowest possible risk when processing personal data,
the following protective measures are implemented, among others:

- Minimize the amount of personal data

- Pseudonymize or encrypt data as early as possible
- Establish transparency with regard to the functions and processing of data
- Delete or anonymize data as early as possible
- Minimizing access to data
- Preset existing configuration options to the most privacy-friendly values

4.6 Order control

The aim of order control is to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

All subcontractors are selected according to defined criteria and are obliged to comply with the GDPR. A list of subcontractors is available.

Service providers acting as processors within the meaning of the GDPR are selected with the utmost care according to data protection criteria. These are contractually bound to the client in accordance with Art. 28 GDPR. The technical and organizational measures for the protection of personal data specified in the contractual agreement are based on the standards described in this document. A list of processors is available.

Employees receive regular training in data protection law. They are therefore familiar with the client's right to issue instructions with regard to commissioned data processing, both in their role as client and in their role as contractor.
Persons authorized to issue instructions on the part of the client are named and known to the contractor.

The contractor's IT security is assessed before the contract is awarded.

This is ensured by clear contract design with a definition of the rights and obligations of the parties, using formalized contracts and order forms. The execution of contracts is regularly reviewed and monitored. Instructions are always accepted in writing and with written confirmation.

No order data processing within the meaning of Art. 28 GDPR takes place without a corresponding instruction from the client, e.g.: Clear contract design, formalized order management, strict selection of the service provider, obligation to obtain prior approval, follow-up checks.

All activities are based on an order from a customer. At a minimum, an existing contract applies. Standard changes, insofar as personal data is processed, are only accepted by authorized persons of the customer.