gridscale

Information about technical and organizational measures (TOM) according to Art. 32 GDPR

Table of Contents

I. Confidentiality (Art. 32 Abs. 1lit. b GDPR)

Access control

The following topics have been considered for security reasons (from outside to inside)

Access to the data center is only possible through a permanently guarded entrance area and only for persons who are on an access authorization list or have been registered. The server room itself is located in an indoor area and is protected against unauthorized access by an access control system. Authorized employees can open the door by using a PIN code in conjunction with an access card.

The authorizations are managed/authorized by the "Head of Security" and are documented in the data center portal.

Sufficiently secured entrances

The entrances to the data center are locked at all times and a porter sits at the main entrance. All doors to the building, the floors, the rooms on the floor and access to our data center area are always locked and secured with an electronic door lock.

There are no light shafts available, no ventilation openings, no windows, and there is no fire escape ladder.

There is a fire stairway at both ends of the building.

All doors have electric door openers with access control.

Guarding

The data center site is guarded around the clock and also the data center gate is occupied around the clock.

The area of the data center and the interior are monitored by cameras.

Written regulation and instructions

Badges are used as keys and must be collected from reception in the data centre after prior registration and can then be used to gain access. These access authorisations are documented and regulated in the data centre operator's portal.

Monitoring of devices to ensure access control for critical security areas, such as for server rooms.

Access is controlled manually by the gatekeeper at the entrance and by video surveillance. The server room is secured with a numerical code in conjunction with the "badge". After three incorrect entries, access is blocked for 15 minutes.

There is a video surveillance of all corridors, in every building and in the entire data centre.

Conditions for access authorization

There is a visitor book at the main entrance for recording visitor data and issuing a visitor badge to authorized persons.

There is a separation of processing and public zones. Visitors register at the main entrance to receive a visitor badge before they are allowed to enter the data center.

Visitors must be registered in advance via the data center operator's portal. They then report to the main entrance to receive a visitor badge on presentation of an ID document before they are allowed to enter the data center. Visitor authorizations must be issued in advance by authorized persons.

Safety consideration for work places at

There are written instructions for mobile working. We do not have any BYOD devices.

Entries are documented

Access for cleaning staff must be requested/authorized on the portal of the data center operator.

Access for maintenance personnel must also be requested/authorized on the portal of the data center operator.

Access for security escorts must also be requested/authorized on the portal of the data center operator.

Access control

User identification and password procedure are defined

No proper noun and words from the dictionary special characters must be used, the minimum password length is fourteen digits or more.

The password guideline is documented in the gridscale information security guideline.

Policy for a tidy working environment and screen locks

The auto-logout (similar to screen lock) has been rolled out automatically on all servers.

A blocking access in the event of more than three login failures, is either standard or otherwise technical impossible. There is a "Clean Desk Policy" in the whole company.

Creation of a user master record per user

Passing on passwords is prohibited

Encryption of data disks

Access control

Protection against unauthorized internal and external access through

All servers are technically positioned behind several redundant firewalls.

The standard security concept of Linux is built in such a way that no virus scanner is necessary. Regular maintenance also ensures that viruses have no chance because the software is always up to date.

The Microsoft solution is used for Windows systems. All documents are either stored in cloud-based solutions or are backed up accordingly to enable recovery if necessary.

Protection against unauthorized internal and external access, encryption through

Design of the authorization concept and the access rights

For users and Administrators, there is a central instance, for assigning authorizations, based on a role model.

Regulations for monitoring and logging

Accesses or access attempts are logged.

The evaluation of the logs processed through automated analysis and notification.

The storage of logs is in a period of 3 - 12 months, depending on the respective system.

Written documentation of data medias

Type and amount storage devices are documented.

Data carriers are stored in a steel cabinet on site in the data center, in a locked room.

Data device management

There is a record of incoming and outgoing data carriers and an inventory as well as a regular data carrier inventory.

Regulation for handling of data medias

The area in which data carriers may be located is defined.

The person, who is authorized to remove data medias are determined.

Regulation for data device usage

The use of external storage media is prohibited.

Handling of data medias is regulated

The storage of obsolete data carriers or data carriers to be destroyed and their destruction is defined in a process.

Destruction is carried out by a certified provider.

The disposal company is certified.

Pseudonymisation

Personal data pseudonymisation

"Pseudonymisation" is defined in Art. 4 No. 5 GDPR as "the processing of personal data in such a way that the personal data can not be assigned to a specific data subject without additional information, provided that this additional information is kept separately and technical and organizational measures that ensure that the personal data are not assigned to an identified or identifiable natural person."

These data are stored separately to the pseudonyms.

A non-allocation is ensured by technical and organizational measures. After a cancellation, the user account will be immediately and irrevocably deleted and removed directly from the database, if no provided statutory retention periods.

The proof of cancellation will be kept for 90 days and after 90 days the proof of cancellation will also be permanently deleted.

There is an independent right-roll concept for de-pseudonymisation.

Separation bid

Implemented separation bidding

Test and development environments, as well as the operating environment, are separated from each other. There is no direct data exchange between the individual environments. The types of test environments depend on the test run and test type and range from unit tests in automatically provided test containers to hardware staging in which integration tests of individual components are carried out. The processes were documented accordingly.

Regulation of separation

The separation is done by a physical solution through, separate server hardware and by a virtualized solution with VLAN/switches.

Separation of mandates on the systems

To follow the data protection compliant ensured for multi-client capability, virtualization of the individual customer machines is used (kernel-based virtual machine) and virtualization software is employed. This achieves a separation of the individual virtual machines, which also prevents unwanted interaction between the VMs and thus isolates them.

To ensure data protection-compliant purpose limitation, data is processed and documented in accordance with the processing directory.

Ensuring data protection compliance

Processing is completely separated by a software, a hardware and a virtualization layer.

II. Integrity (Art. 32 Par. 1lit. b GDPR)

Relay control

Transmission

Via data line via VPN and HTTPS.

Ensured privacy

By secure delivery, VPN (Virtual Private Network).

Input control

Privacy-compliant input control

By logging and evaluation logging systems: recorded in the respective log file, but not analysed.

The retention period of the logs will be retained and deleted in accordance with the legal basis and legitimate purpose of processing.

III. Availability and resilience of systems and services (Art. 32 Par. 1lit. b GDPR)

Availability and resilience

Monitoring of all failure-critical infrastructure systems of the data center

Fire protection equipment and monitoring with automatic, digital fire alarm system. F-90 fire-fighting sections and fire protection walls of fire resistance class F 90.

Fire extinguisher are available in every room.

Smoke detector, Early fire detection systems (smoke aspiration system - RAS), which are integrated into a fire alarm system, ensure the earliest possible detection.

Fire detector with automatic monitoring and digital fire alarm system.

The fire is extinguished by an automatically controlled fire extinguishing system.

High water protection devices are not required for the server room, which is located on the 1st floor.

Smoking is prohibited in the entire data center.

Redundant power supply facilities are available with separate UPS systems (A and B supply).

An emergency power generator are solved by redundantly designed emergency power systems with diesel generators.

An uninterruptible power supply (UPS) through separate UPS systems (A and B supply).

The hard drives are protected by a RAID system.

Concept for regular backup

Backup data carriers are stored separately or the data backup is stored at a different geographical location.

Data backups are made where necessary, as daily backups, monthly backups or annual data backups, based on a documented backup procedure, automatically processed.

Is the resilience of the systems and services regularly performed or tested.

Resistant IT systems are called, for which are also resistant, even for DDoS-attacks. In this sense, resilience means robustness.

Concept for regular Security-Updates

Updates are installed weekly, monthly or when required immediately, depending on the system.

IV. Rapid recoverability (Art. 32 Par. 1 lit. c GDPR)

Rapid recoverability

Checklist for checking the emergency concept

A security concept, based on this risk analysis, has been developed for possible disruptions e.g. technical defects, fire, sabotage, forces of nature etc., and implemented.

This concept adapted on an ongoing basis (at least annually) to the changed circumstances. An audit plan has been drawn up that provides for a review of the document min. once a year.

Identified vulnerabilities were eliminated. An emergency power supply is available and an overvoltage protection has been installed.

It has been documented, what hardware will be needed, in case of emergency. Each hardware is designed to be redundant and was purchased and implemented precisely for this purpose.

A mirroring of the most important files, to another storage medium, exists.

The availability of employees, to have to be alarmed (for example system responsible, operating, data center manager, database administrator etc.) is guaranteed.

The required system passwords have been deposited, at a secure location.

The availability of maintenance technicians and hardware replacement parts has been regulated, by the conclusion of a maintenance contract, with the manufacturer. The failure of one component does not result in a loss of service for the customer. The service is manufacturer-independent.

The data lines have multiple redundancies.

The need for the most necessary peripherals (screens etc.) has been regulated.

An archive has been set up for the outsourcing of backup media.

The availability of these data medias are guaranteed in an emergency case.

The restart, of an emergency operation for main procedures (according to the pre-established priority list) or full data processing is within a reasonable period of time possible.

The documented description of the recovery measures and processes exists.

The necessary measures are known to the persons concerned.

Corresponding measures are checked and tested regularly (at least every six months).

The above checkpoints are documented in writing.

V. Procedure for regular review, evaluation and validation (Art. 32 Par. 1lit. d GDPR; Art. 25 Par. 1 GDPR)

Review of technical and organizational measures

Accountability (Article 5 (2) EU GDPR)

Organizational structure

A data protection guideline is available in the company and announced to employees.

A data protection officer has been appointed and reported to the supervisory authority.

Reporting confirmation date is available in writing was 01.11.2021.

The duties of the Data Protection Officer are defined.

The data protection officer supports the management in an advisory capacity and the departments.

As well as responsible for the control of the sensitization of the employees. DSGVO / GDPR training is provided during on-boarding and there are several refresher and further training courses each year.

Audits and inspections are carried out and documented as part of the audit plan. The annual ISO audits are carried out, documented and evaluated by an external certification body.

The response/clarification of data protection complaints is escalated organizationally to the management or to the data protection officer.

Requests from data subjects are either sent to compliance@gridscale.io or escalated to the management or forwarded to the data protection officer. Appropriate templates have been created to respond to such requests.

Reporting and notification of data breaches (Art. 33/34 GDPR), is controlled and executed by a "Data Breach Procedure" (SOP-60).

Uniform data protection concept for all sites is available.

Concept for tasks / training on data protection is built. All employees receive refresher training on data protection and data security several times a year.

Rules for internal controls are defined and with ISO 27001 / 27018 regularly audited and reviewed in accordance with the audit plan.

Rules for handling of data protection reports are created. The data protection report is published once a year and made available to the management.

Regulations for the cooperation of the departments with the DPO are defined. The management is aware of the need to implement the GDPR requirements, e.g. in programs, data economy, security by design, etc. and consults the DPO if necessary. In addition, the Sales department ensures the fulfillment of corresponding contractual requirements such as AVV, TOMs etc. with the customer. This is reinforced, for example, in regular training and information sessions.

Basic-Requirements:

A list of processing activities (Article 30 of the GDPR) is created and up-to-date.

Uniformed risk model has been implemented.

Privacy compliant processing is implemented.

Dealing with affected rights is implemented.

Dealing with data breaches is implemented.

The use of subcontractors and third-party specialist services are documented.

If a contractor acts as a processor pursuant to Art. 28 of the GDPR, the contractor shall process personal data only in accordance with the contractual requirements of the client.

In the case of additional orders, e.g. "remote hands", which include or cannot exclude the processing of or physical access to data carriers of personal data, separate contracts in accordance with GDPR Art. 28 shall be concluded if necessary or existing contracts shall be supplemented.

Where necessary, data protection-compliant contracts are concluded with subcontractors in accordance with GDPR Art. 28. The selection of service providers is made carefully.

gridscale GmbH