

Annex – Technical and organizational measures in accordance with Art. 32 GDPR

Status: 25. März 2025

fino data services GmbH
Universitätsplatz 12, 34127 Kassel

§ 1 Confidentiality (Art. 32 para. 1 lit. b GDPR)

1.1. Access control

Measures that are suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data is processed or used.

fino's offices are not a production site in the true sense of the word. The productive application runs exclusively in ISO-27001 certified data centers.

(a) Fino offices

fino's premises are adequately secured against unauthorized access by the following measures:

- Building used exclusively for commercial purposes;
- All entrances are secured against unauthorized access by the following measures:
 - Doors are always locked;
 - Security locks;
 - Key registered on a personal basis;
 - Documented key issue;
 - Personalized transponder-based locking system;
 - The access record is read out from the locking system if necessary
 - Visitors can only move around when accompanied by staff;

(b) Data center

The data centers are adequately secured against unauthorized access, in particular by the following measures:

- Access to the data center only for authorized persons after prior registration
- Access security through a material (RFID chip) and a mental (PIN) identification feature: A distinction is made between permanently assigned access authorizations and access authorizations deposited with the security service for collection. In the case of access authorizations deposited for collection, authorization is ensured by checking the ID card. The data is stored with a security service (whitelist) to ensure that only authorized persons can enter the data center;
- Access to the individual customer lockers or areas is only possible by the customer and the responsible personnel;
- the access control systems and the alarm systems are protected against power failure via UPS and emergency power system;
- Video surveillance

- Perimeter protection
- Security service: the data center is regularly inspected by a security service within specified time windows. The points to be checked by the security service in the data centers are defined. Any anomalies are reported. The specified routes taken by the security staff are logged.

1.2. Access control

Measures that are suitable for preventing data processing systems from being used by unauthorized persons.

Authenticated user identification is carried out, in particular in that:

- all technical systems (centralized and decentralized), hardware and software are firewall-protected
- access to servers is only granted to a limited number of people.
- Employees can only access servers using their personal SSH key. These employee SSH keys must be explicitly activated on each server; all access is deactivated when an employee leaves the company.
- Clear assignment of user accounts to users, no impersonal collective accounts (e.g. "Employee-1")
- Temporary brute force prevention after failed login attempts
- mobile data carriers (laptops and smartphones) are encrypted separately
- The use of mobile devices is regulated by employee agreements
- Every work computer is password-protected. Password regulations are set out in a password policy.
- Each work computer is locked when you leave the workstation; automatic password-based screen and computer lock after 15 minutes of inactivity
- Authorizations for external employees are temporary and limited to developer platforms;
- External employees and visitors use the guest WLAN

1.3. Access control

Measures that ensure that persons authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage.

Unauthorized activity in data processing systems outside of granted authorizations is prevented in particular by the fact that:

- the access rights (both for users and administrators) are based on the task-related and data protection requirements;
- every access to applications (entry, modification and deletion) is logged and can be evaluated (for at least one year: the log data is deleted at the end of the year following its generation in accordance with Section 76 (4) BDSG);
- protection against unauthorized internal and external access through encryption and firewalls.
- Separation of development, test and production operation at the hypervisor level and communication of the virtual machines via a VPN tunnel, whereby no access between the systems is possible

1.4. Separation requirement

Measures to ensure that data collected for different purposes can be processed separately.

- physically separate storage on separate systems or data carriers
- Logical client separation (on the software side)
- Separation of production and test system

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

The processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures;

The processing of personal data in compliance with the requirements of pseudonymization in accordance with Art. 32 para. 1 a GDPR is ensured in particular by the following measures:

- Internal rules on pseudonymization
- Commitment of employees
- Technically automated implementation of the rules and regulations
- Code changes to the pseudonymization process can only be merged after separate approval
- Control through unannounced spot checks

§ 2 Integrity (Art. 32 para. 1 lit. b GDPR)

2.1. Transfer control

Measures to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transmission or during transport or storage on data carriers, and that it is possible to verify and establish to which bodies personal data are intended to be transmitted by data transmission equipment.

The aspects of the transfer control of personal data are implemented by the fact that:

- data communication is encrypted in accordance with TLS and VPN technology is used;
- There is a constantly updated firewall and virus protection concept on the server side, and end devices are secured in line with standard market practice.
- Email messages are always sent in encrypted form. Other information is - where possible - anonymized before being passed on and is not transmitted in a personalized form;
- There are no plans to store personal data on data carriers outside the data center. Physical transportation of data carriers with personal data does not take place.

2.2. Input control

Measures that ensure that it is possible to subsequently check and determine whether and by whom personal data has been entered, modified or removed from data processing systems.

(a) Products without data storage

fino processes the end customer's data without storing it persistently. During processing by the end customer, the data is only available on their input device. Employees do not have access to personal data at any time and therefore cannot change it. Upon completion or commissioning of the process, the required data is temporarily held in a queue for any automated further processing or letter/fax/mail dispatch. Once the purpose has been achieved, e.g. successful processing and dispatch of all documents, all documents and the order data are deleted in the automated process.

(b) Products with data storage

For products that require data to be saved, every entry, change and deletion by the application is clearly assigned to a user login. Logging of all administrative write accesses at database level is active, whereby the time stamp and the action are logged.

The log data of the respective applications is stored in a central logging system (Sematext).

§ 3 Availability and resilience (Art. 32 para. 1 lit. b and c GDPR)

Measures to ensure that personal data is protected against accidental destruction or loss and can be recovered quickly.

Data storage within a cloud architecture has multiple redundant backups and is itself fail-safe. Daily backups are created as hard disk snapshots in multiple mirroring, which can be restored at any time as a replacement for a running system. The systems are continuously monitored and load balancing measures are implemented in the event of load peaks. If a server fails, it is restarted with the help of self-healing.

§ 4 Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

- Privacy-friendly default settings:
 - The factory settings of the applications are selected so that only the data required to fulfill the purpose of the application is collected.
 - Voluntary additional information provided by the user is marked accordingly.
- data protection management system:
 - Overall Group-wide measures for the protection of personal data
 - Data protection organization and responsibilities, involvement of the data protection officer, list of processing activities, deletion concept, data protection impact assessment, contract management, employee obligations, data protection training, process for exercising data subject rights, process for reporting data protection violations
- Incident Response Management:
 - Process for recording, categorizing, prioritizing and resolving detected or suspected faults and security incidents
 - Fastest possible restoration of the service
 - Informing the affected stakeholders
- Definition of competencies and control measures in coordination with the client and integration of the same into the operational processes
- Obligation of employees to comply with the GDPR, telecommunications secrecy (Section 3 TDDDG), professional secrecy (Section 203 StGB) and banking secrecy.
- Ensuring the destruction of data after completion of the order
- Written instructions between contractor and client by means of a data processing agreement within the meaning of Art. 28 GDPR
- Selection of contractors under due diligence aspects (in particular with regard to data security)
- prior inspection and documentation of the safety measures taken by the contractor

Status: March 25, 2025