Technical and organizational measures (TOM)

According to Art. 32 GDPR

This document describes the technical and organizational measures implemented by EGI Foundation to meet legal and contractual requirements when processing personal data.

The measures described in numbers 1 to 13 serve the purpose …

- to encrypt or pseudonymize personal data where necessary (see, inter alia, 6 to 8),
- to ensure the confidentiality, integrity, availability and resilience of systems and services in connection with the processing of personal data (see, inter alia, 1 to 10),
- to restore the availability of and access to personal data in the event of a physical or technical incident in a timely manner (see 11), and
- to regularly review, assess and evaluate the effectiveness of all technical and organizational measures to ensure the security of processing (see, inter alia, 12 and 13).

The following measures apply to all data processing activities that are under control of EGI Foundation, or where EGI Foundation is a subcontracted data processor on behalf of another data controller.

In situations where EGI Foundation is the data controller and another organization is the data processor on behalf of EGI Foundation, EGI Foundation aims at ensuring that the technical and organizational measures implemented by the subcontracted processor equals at minimum the processing security level indicated by following measures.

Please note: In federated service delivery scenarios, one or more data controllers and one or more subcontracted data processors may be entrusted with or involved in processing personal data.

(1) Access control

All access rights (both for access to IT systems and data and for access to buildings and rooms) are assigned according to the principle that employees and third-party users are only granted the level of access they need to perform their activities (need-to-know principle).

Access rights are granted according to defined (role-based) permission profiles. The access rights granted are reviewed regularly. Rights that are no longer required are withdrawn immediately.

Access to networks and network services is restricted by technical and physical measures. Access to wireless corporate networks that allow access to personal data is protected by personalized authentication (PKI, IEEE 802.1x). This applies in an analogous manner to wired access, unless it is from a secure area that is sufficiently protected and controlled by physical access control measures.

(2) Physical access control

Physical secure areas (zones) are defined on the basis of information security and data protection requirements and protected against unauthorized access by appropriate physical

safeguards. The physical security concept distinguishes between public areas, controlled areas, restricted/internal areas, and high-risk zones. Secure zones are defined based on the protection needs of the information assets housed or made accessible within them.

Depending on the specific zone classification, selected or all of the following security features are implemented: Access restriction through personalized access medium, video surveillance and door-open sensors at access points, motion detection, privacy screens or view guards on potentially confidential information, and no photography policy.

For dealing with visitors and deliveries, procedures are used to prevent unauthorized persons from accessing security areas.

(3) Logical access control to processing systems

All data processing systems are equipped with a secure authentication mechanism (X509 certificate or password protection).

Defined procedures are used to authorize access to information, taking into account the need-to-know principle. Special procedures are in place for granting access rights to privileged systems (e.g., systems or applications used to control or administrate critical processes or to manage access rights for other systems).

For authentication on data processing systems (IT systems), secure passwords are used that have sufficient length, are robust against dictionary attacks, do not contain strings of consecutive letters or digits and are not based on facts that could be easily be guessed by others. Passwords must be changed whenever there is an indication that the password has been compromised. A changed password must not match or contain a password that has been used in the past. Where technically possible, the use of two-factor-authentication is enforced.

A " clear desk & screen policy" is implemented: When leaving the workplace, all computers in use must be locked (screen lock). In case of inactivity, the screen lock is automatically activated after a maximum of 10 minutes. Documents that may contain confidential information must not be kept open and unattended on desks or in other freely accessible storage areas.

(4) User activity control

All employees must attend mandatory basic training on information security and data privacy on an annual basis. Participation in this training is recorded. New employees are familiarized with the main regulations on information security and data privacy relevant to them at the start of their employment or assignment.

User activities, including logon attempts to data processing systems (IT systems), are logged to the extent required.

User accounts via which personal data can be accessed as part of processing activities must be personalized and must not be shared by more than one person.

Administrative activities on IT systems (such as changes to system configurations) are logged. Configuration files are historized, backed up and checked regularly and as required.

(5) Segregation control

It is ensured that personal data collected for different purposes are not mixed in their processing. To this end, multitenant systems are used where necessary, or systems are physically or logically separated.

(6) Data carrier and mobile device control

Data carriers containing personal data are stored in secure locations that prevent access to these carriers by unauthorized persons.

Personal data stored on mobile devices and data carriers (including laptops, smartphones, USB sticks) are required to be encrypted. The use of any type of private Internet/Cloud storage for the (temporary) storage of such data is prohibited. Confidential data will never be stored on private storage media or end devices.

Personal data that are no longer required are deleted. Electronic storage media and paper documents that are no longer required will be disposed of or destroyed / made unusable in such a way that it is no longer possible to gain knowledge of the data stored or contained on them.

The use of mobile devices is restricted and controlled. If personal data are accessed via mobile devices, suitable measures are taken to ensure that the devices cannot be used by unauthorized persons, for example in the event of loss or theft. All mobile devices used for business purposes are configured in such a way that they are protected by a query for a secret (e.g., PIN, pattern or biometric information) in the lock screen. The lock screen is automatically activated during inactivity. The corresponding mobile devices must never be left unattended. Modifications to the operating system software / firmware are prohibited. Security-relevant updates and patches are applied automatically. The devices are subject to comprehensive mobile device management (MDM), which technically implements these and other restrictions, policies, and measures.

(7) Pseudonymization and anonymization

Measures for pseudonymization or anonymization of personal data are implemented to the extent necessary. Data in development environments used for testing purposes is anonymized or pseudonymized wherever possible. Data on the usage of websites that is evaluated to generate usage statistics is anonymized.

(8) Transfer and dissemination control

Mechanisms for securing data traffic and communication connections, as well as for monitoring and logging activities in networks, have been established to the required extent. As appropriate, firewalls and intrusion detection and prevention systems (IDS / IPS) are in place.

When personal data is transmitted via public communication networks, secure end-to-end encryption of the communication is ensured. When establishing secure connections (VPN tunnels) offering access to IT resources via public networks, two-factor authentication is used as a matter of principle. If the exchange of confidential authentication information is required, this is done via a different communication path than the actual data transmission.

When transporting personal data stored on data carriers, the use of encryption, among other things, ensures that the data is protected against unauthorized access, manipulation or loss. After transport, the data is deleted from the storage media used for transport if it is no longer required on them.

Paper printouts and exports of confidential data from their source system are avoided whenever possible. Hard copies and electronic exports of confidential information leaving the business premises are handled with special care, taking into account the relevant confidentiality level - with the aim of preventing disclosure, loss and unauthorized copying. As soon as a paper printout is no longer required, it is destroyed. Electronic data exports that are no longer required are deleted again from the respective storage location and any transport data carrier used.

(9) Input control

Measures for subsequent verification of whether and by whom data has been entered, changed or removed (deleted) are implemented to the extent necessary. In systems used to collect and process personal data, access is categorized and automatically recorded. The integrity of log information is ensured.

(10) Availability control

A redundant design of communication and data processing systems (IT systems) and supporting facilities has been implemented to the required extent. An uninterruptible power supply (UPS) and high-availability Internet connection with automatic failover have been implemented at all relevant locations. Server and storage systems are designed redundantly (including redundant power supply units, disk mirroring). As appropriate, load balancing and failover are implemented for virtualized server systems.

(11) Recoverability

Data backups of databases and operating system images are taken to the extent required and with the aim of preventing the loss of personal data in the event of a technical malfunction or human error. Backups are performed for network drives and servers in productive operation, and the performance is recorded (logged) and monitored. The recovery of data backups is tested.

Processes or procedures for handling disruptions to IT systems and for restoring systems after a disruption have been established to the extent required.

Business continuity management (BCM) includes activities for business process impact analysis (BIA), definition and application of measures to ensure business continuity, taking into account information security and data protection aspects, as well as tests and reviews of the effectiveness of the measures implemented. A business process impact analysis is prepared or reviewed at least annually on the basis of the key business processes and services.

(12) Job control and subcontracting

The selection of subcontractors is carried out with the objective of ensuring that there is no increased risk to compliance with data protection objectives.

Depending on their role and the scope of access to confidential or personal data, subcontractors must, among other things, acknowledge and comply with regulations on secrecy / confidentiality as well as data protection (e.g., confidentiality / non-disclosure agreement), as well as an information security policy for suppliers.

In the case of security-critical subcontractors, service providers or suppliers, the following reporting and audit requirements are implemented: evaluation of contractually agreed reports (e.g., security events/incidents, availability statistics) as well as supplier audits using a self-assessment questionnaire, with an additional on-site inspection as necessary.

(13) Review, assessment and evaluation

Information on potential technical vulnerabilities or errors in data processing systems (IT systems) is evaluated at regular intervals and appropriate measures are initiated. Critical patches are deployed for both operating systems and software applications in use.

Data processing systems (IT systems) are checked regularly to the extent required and after changes to ensure that they are functioning properly.

An internal audit program is in place that covers regular system audits, process audits, IT security audits and data protection audits and controls.