Cologne, 18.01.2022

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):

Sufficiently secured entrances:

Guarding:

Written regulation, instruction:

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

Conditions for access authorization:

Safety consideration for work places:

Entries are documented:

Access control

User identification and password procedure:

Automatic locking of screens:

Creation of a user master record per user

Passing of password is not allowed:

Encryption of data disks

Access control

Protection against unauthorized internal and external access, firewall

Protection against unauthorized internal and external access, encryption:

Design of the authorization concept and the access rights:

Regulations for monitoring and logging: ; - storage of logs between 30 days to 12 months and depends on the system

Written documentation of data medias set:

Data device management:

Regulation for handling of data medias:

Regulation for data device usage:

Handling of data medias is regulated:

Pseudonymisation

Are personal data pseudonymised?

"Pseudonymisation" is defined in Art. 4 No. 5 DS-GVO 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."

Separation bid

Implemented separation bidding:

Regulation of separation:

Separation of mandates on the systems:

Ensuring data protection compliance:

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

Relay control

Transmission: - via data line

Ensured privacy by: - secure delivery, VPN (Virtual Private Network)

Input control

Privacy-compliant input control:

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

Availability and resilience

Monitoring of critical areas and critical infrastructure systems:

Concept for regular backup:

Is the resilience of the systems and services regularly performed or tested by: (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, depending on the system.

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

Rapid recoverability

Checklist for checking the emergency concept

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:

Data protection guideline

Data protection officer has been appointed and reported to the supervisory authority

Duties of the Data Protection Officer are defined

Uniform data protection concept for all sites

Concept for tasks / training on data protection

Rules for internal controls

Rules for handling of data protection reports

Regulations for the cooperation of the departments with the DPO

Basic-Requirements

List of processing activities (Article 30 of the GDPR)

Uniformed risk model

Privacy compliant processing

Dealing with affected rights

Dealing with data breaches

Use of subcontractors

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 DS-GVO 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 DS-GVO Art. 28. The selection of service providers is made carefully.

With kind regards

gridscle GmbH