Chancental Works GmbH
Zinggenstrasse 15
CH-9434 Au/SG
Switzerland

Technical and organizational measures (TOM) within the meaning of Art. 32 GDPR

Table of contents

1 Preliminary remark

All personal data of Chancental Works GmbH is stored and processed exclusively in external data centers.

The following information refers to the system environments used.

Chancental Works GmbH does not have its own server room.

Third parties or Chancental Works GmbH staff do not have access to the infrastructure used.

2 Confidentiality in accordance with Art. 32 (1) lit. GDPR

2.1 Access control

Measures that are suitable for preventing unauthorized persons from accessing data processing systems that process or use personal data.

Technical measures	Organizational measures
☒ Alarm system	☒ Key policy/list
☒ Automatic access control system	☒ Reception / front desk / doorman
☒ Biometric access barriers	☒ Visitor log / visitor log
☒ Chip cards / transponder systems	☒ Employee/visitor ID cards
☒ Manual locking system	☒ Visitors accompanied by employees
☒ Doors with knobs on the outside	☒ Careful selection of security personnel
☒Doorbell system with camera	☒ Careful selection of cleaning services
☒ Video surveillance of entrances	

2.2 Access control

Measures designed to prevent data processing systems from being used by unauthorized persons.

Technical measures	Organizational measures
☒ Login with username + strong password	☒ Manage user permissions
☒ Anti-virus software server	☒ Create user profiles
☒ Anti-virus software clients	☒ Central password assignment
☒ Anti-virus software for mobile devices	☒ "Secure password" policy
☒ Firewall	☒ "Delete/Destroy" policy
☒ Intrusion detection systems	☒ Clean desk policy
☒ Use of VPN for remote access	☒ General data protection policy and/or security
☒ Encryption of data carriers	
☒ Encryption of smartphones	
☒ Automatic desktop lock	
☒ Encryption of notebooks/tablets	
☒ Intrusion prevention systems	
☒ Two-factor authentication in data center operations and for critical systems	

2.3 Access control

Measures that ensure that those authorized to use a data processing system can only access the data for which they have access authorization, and that personal data cannot be read, copied, modified, or removed without authorization during processing, use, and after storage.

Technical measures	Organizational measures
☒ Document shredder (at least level 3, cross cut)	☒ Use of authorization concepts
☒ Physical deletion of data carriers, security level H-4 (DIN 66399)	☒ Minimum number of administrators
☒ Logging of access to applications, specifically when entering, modifying and deleting data	☒ Management of user rights by administrators
☒ Access to systems via SSH	☒ Application of cryptographic methods in line with the current state of technology
☒ TLS encryption	

2.4 Separation control

Measures that ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of the data.

Technical measures	Organizational measures
☒ Separation of production and test environments	☒ Control via authorization concept
☒ Physical separation (systems / databases / data carriers)	☒ Definition of database rights
☒ Multi-client capability of relevant applications	☒ Defined requirements `for` development environments
☒ VLAN segmentation of networks	
☒ Logically separated customer systems	
☒ Staging of development, test, and production environments	

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

Technical measures	Organizational measures
☒ In the case of pseudonymization: Separation of assignment data and storage storage in separate and secure systems (encrypted if possible) secure system (encrypted if possible)	☒ Internal instruction to anonymize/pseudonymize personal anonymize/pseudonymize personal data in the event of disclosure or even after the expiry of the statutory deletion period

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

3.1 Transfer control

Measures to ensure that personal data cannot be read, copied, modified, or removed without authorization during electronic transmission or input, during transport, or during storage on data carriers, and that it is possible to verify and determine to which locations personal data is to be transmitted by data transmission facilities.

Technical measures	Organizational measures
☒ Email encryption	☒ Documentation of data recipients and the duration of the planned transfer or deletion periods
☒ Use of VPN	☒ Overview of regular retrieval and transmission processes
☒ Logging of accesses and retrievals	☒ Implementation of the need-to-know principle
☒ Provision via encrypted connections such as sftp, https – Secure cloud stores	

3.2 Input control

Measures that ensure that personal data cannot be read, copied, modified, or removed without authorization during electronic transmission or input, during transport, or during storage on data carriers, and that it is possible to check and determine where personal data is to be transmitted by data transmission facilities.

Technical measures	**Organizational measures**
☒ Technical logging of input, modification, and deletion of data	☒ Overview of which programs which data can be entered, modified, or deleted
☒ Manual or automated control of the logs	☒ Traceability of input, modification, and deletion of data through individual usernames (not user groups)
	☒ Assignment of rights for entering, modification, and deletion of data based based on an authorization concept
	☒ Clear responsibilities for deletion

4 Availability and resilience (Art. 32 (1) (b) GDPR)

4.1 Availability control

Measures to ensure that personal data is protected against destruction or loss (UPS, air conditioning, fire protection, data backups, secure storage of data carriers, virus protection, RAID systems, disk mirroring, etc.).

Technical measures	**Organizational measures**
☒ Fire and smoke alarm systems	☒ Backup & recovery concept (formulated)
☒ Fire extinguishers in server room	☒ Control of the backup process
☒ Server room monitoring Temperature and humidity	☒ Regular tests for data recovery and logging of results
☒ Air-conditioned server room	☒ Storage of backup media in a secure location outside the server room
☒ UPS system and emergency diesel generators in the data center	☒ No sanitary connections in or above the server room
☒ Protective power strips in server room	☒ Existence of an emergency plan (e.g., BSI IT-Grundschutz 100-4)
	☒ Regular testing of diesel generators in the data center
☒ RAID system / hard disk mirroring	
☒ Video surveillance in server room	
☒ Alarm message in case of unauthorized access to server room	
☒ Use of protection programs against malware	

4.2 Recoverability

Measures that enable the availability of personal data and access to it to be quickly restored in the event of a physical or technical incident.

Technical measures	**Organizational measures**
☒ Backup monitoring and reporting	☒ Recovery concept
☒ Restorability from automation tools	☒ Control of the backup process
☒ Backup concept based on criticality and customer specifications	☒ Regular data recovery tests and logging of results
	☒ Storage of backup media in a secure location outside the server room

5 Procedures for regular review, assessment, and evaluation (Art. 32 (1) (d) GDPR; Art. 25 (1) GDPR)

5.1 Data protection management

Technical measures	Organizational measures
☒ Central documentation of all data protection regulations with technical access for employees	☒ Data protection management system implemented
☒ An annual review of the effectiveness of technical protection measures	☒ Information security management implemented
☒ Security certification according to ISO 27001	☒ Data protection impact assessment (DPIA) is carried out as required
☒ Data protection management system in accordance with ISO 27701	☒ The organization complies with the information obligations under Articles 13 and 14 of the GDPR
☒ The effectiveness of the technical protection measures is reviewed annually	

☒ Incident response management

5.2 Incident response management

Support in responding to security breaches and data breach processes.

Technical measures	Organizational measures
☒ Use of firewalls and regular updates	☒ Documented procedure for dealing with security and data protection incidents
☒ Use of spam filters and regular updates	☒ Documentation of security incidents and data breaches via ticket system
☒ Use of virus scanners and regular updates	
☒ Intrusion detection system (IDS)	
☒ Intrusion prevention system (IPS)	

5.3 Privacy-friendly default settings (Art. 25(2) GDPR)

"Privacy by design" / "Privacy by default" in accordance with Art. 25 (2) GDPR

Technical measures	Organizational measures
☒ No more personal data is collected than is necessary for the respective purpose	
☒ Consideration of the principles of "data protection by design" and "Data Protection by Default" ("Data Protection by Default") are taken into account in software development	

5.4 Order control (outsourcing, subcontractors, and order processing)

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

Technical measures	Organizational measures
☒ Monitoring of remote access by external parties, e.g., in the context of remote support	☒ Supplier evaluations are carried out on a risk-based basis
☒ Monitoring of subcontractors in accordance with the principles and technologies described in the preceding chapters	☒ Prior review of the security measures taken by the contractor and their documentation
	☒ Selection of the contractor based on defined criteria
	☒ Conclusion of the necessary agreement for Order processing
	☒ Regular review of the contractor and its level of protection

6 Technical and organizational measures Subcontractors providing infrastructure

Chancental Works GmbH uses data center service providers as subcontractors in an operational and business management sense.

These are not "further processors" within the meaning of the GDPR, as their core activity does not involve the processing of personal data at any time, but rather a so-called subordinate ancillary service in the form of infrastructure provision.

Due to the relevance of information security for both the contractor and the client—especially with regard to availability—the contractor only uses carefully selected companies for these ancillary activities and checks them regularly.