DPA ANNEX 1

—

TECHNICAL AND ORGANIZATIONAL MEASURES (TOM)

AS OF: MAY 2022

—

The present document supplements the Data Processing Agreement (DPA) between Client and Contractor pursuant to Art 28 GDPR (EU General Data Protection Regulation).

The technical and organizational measures are implemented by Anexia in accordance with Art 32 GDPR. They are continuously improved by Anexia according to feasibility and state of the art - not least also in terms of the active ISO 27001 certification - and brought to a higher level of security and protection.

1. Confidentiality

1.1. Physical Access Control

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

Technical Measures

- ✓ Alarm system
- ✓ Automatic access control system
- ✓ Biometric access barriers
- ✓ Smart cards / transponder systems
- ✓ Manual locking system
- ✓ Doors with knob outside
- ✓ Doorbell system with camera
- ✓ Video surveillance of entrances

Organizational Measures

- ✓ Key regulation / List
- ✓ Reception / Receptionist / Gatekeeper
- ✓ Visitors' book / Visitors' protocol
- ✓ Employee / visitor badges
- ✓ Visitors accompanied by employees
- ✓ Care in selection of security guard personnel
- ✓ Care in selection of cleaning services

The measures refer to the following controls (Annex A) from IEC/ISO 27001:2013: A.11.1 Secure areas, A11.2 Equipment

1.2. Logical Access Control

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

Technical Measures

- ✓ Login with username + strong password
- ✓ Anti-Virus Software Servers
- ✓ Anti-Virus Software Clients
- ✓ Anti-virus software mobile devices
- ✓ Firewall
- ✓ IDS in use (Intrusion Detection Systems)
- ✓ IPS in use (Intrusion Prevention Systems)
- ✓ Use of VPN for remote access
- ✓ Encryption of data carriers
- ✓ Encryption of smartphones
- ✓ Automatic desktop lock
- ✓ Encryption of hard disks for notebooks / tablets / smartphones
- ✓ Two-factor authentication in data center operation and for critical systems

Organizational Measures

- ✓ User permission management
- ✓ Central creation of user profiles
- ✓ Password protected user accounts
- ✓ Application of safety measures for telework according to the state of the art
- ✓ Restricted use of administrative user accounts

The measures refer to the following controls (Annex A) from IEC/ISO 27001:2013: A.6.2 Mobile devices and teleworking, A.9.1 Business requirements of access control, A.9.2 User access management, A.9.3 User responsibilities, A.9.4 System and application access control, A.10.1 Cryptographic controls, A.12.1 Operational procedures and responsibilities, A.12.2 Protection from malware, A.12.4 Logging and monitoring, A.12.5 Control of operational software, A.12.7 Information systems audit considerations, A.13.1 Network security management, A.13.2 Information transfer

1.3. Authorization Control

Measures to ensure that those 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.

Technical Measures

- ✓ File shredder min. recommended security level P-4 (DIN 66399)
- ✓ External destruction of files at least recommended security level P-6 (DIN 66399)
- ✓ Physical deletion of data carriers Security level H-4 (DIN66399)
- ✓ Logging of accesses to applications, specifically when entering, changing, and deleting data
- ✓ SSH encrypted access
- ✓ TLS encryption

Organizational Measures

- ✓ Use of authorization concepts
- ✓ Minimum number of administrators
- ✓ Management of user rights by administrators
- ✓ Application of cryptographic methods according to the current state of the art

The measures refer to the following controls (Annex A) from IEC/ISO 27001:2013: A.8.2 Information classification, A.8.3 Media handling, A.9.2 User access management, A.10.1 Cryptographic controls, A.12.4 Logging and monitoring

1.4. 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

- ✓ Separation of productive and test environment
- ✓ Physical separation (systems / databases / data carriers)
- ✓ Multi-tenancy of relevant applications
- ✓ VLAN segmentation of networks
- ✓ Client systems logically separated
- ✓ Staging of development, test and production environment

Organizational Measures

- ✓ Determination of database rights
- ✓ Defined requirements for development environments
- ✓ Defined requirements for the execution of tests in software development

The measures refer to the following controls (Annex A) from IEC/ISO 27001:2013: A.9.2 User access management, A.12.1 Operational procedures and responsibilities, A.13.1 Network security management, A.14.2 Security in development and support processes, A.14.3 Test data

2. Integrity

2.1. Transfer Control and Input Control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or input or while being transported or stored on data media, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.

Technical Measures

- ✓ Use of VPN
- ✓ Logging of accesses and retrievals
- ✓ Provision via encrypted connections such as sftp, https – secure cloudstores
- ✓ Technical logging of data input, modification and deletion

Organizational Measures

- ✓ Implementation of the need-to-know principle

The measures refer to the following controls (Annex A) from IEC/ISO 27001:2013: A.9.2 User access management, A.10.1 Cryptographic controls, A.12.4 Logging and monitoring, A.13.2 Information transfer

3. Availability and Resilience

3.1. Availability Control

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

Technical Measures

- ✓ Fire and smoke detection systems
- ✓ Fire extinguisher server room
- ✓ Server room monitoring temperature and humidity
- ✓ Server room air-conditioning
- ✓ UPS system and emergency diesel generators DC
- ✓ Protective socket strips server room
- ✓ RAID system / hard disk mirroring
- ✓ Video surveillance server room
- ✓ Use of protection programs against malware

Organizational Measures

- ✓ Existence of an emergency plan
- ✓ Regular testing of the diesel aggregates DC

The measures refer to the following controls (Annex A) from IEC/ISO 27001:2013: A.11.1 Secure areas, A.12.1 Operational procedures and responsibilities, A.12.2 Protection from malware, A.12.3 Backup, A.12.4 Logging and monitoring, A.17.1 Information security continuity, A.17.2 Redundancies

3.2. Recoverability Control

Measures capable of rapidly restoring the availability of and access to personal data in the event of a physical or technical incident.

Technical Measures

- ✓ Backup monitoring and reporting
- ✓ Restorability from automation tools
- ✓ Backup concept according to criticality and customer specifications

Organizational Measures

- ✓ Recovery concept
- ✓ Control of the backup process
- ✓ Regular testing of data recovery and logging of results
- ✓ Storage of backup media in a safe place outside the server room

The measures refer to the following controls (Annex A) from IEC/ISO 27001:2013: A.12.3 Backup, A.12.4 Logging and monitoring, A.17.1 Information security continuity, A.17.2 Redundancies

4. Procedures for regular Review, Assessment and Evaluation

4.1. Data Protection Management

Technical Measures

- ✓ Central documentation of all data protection regulations with technical accessibility for employees
- ✓ Annual review of the adequacy of the TOM

Organizational Measures

- ✓ Data protection management system implemented
- ✓ Information security management implemented

The measures refer to the following controls (Annex A) from IEC/ISO 27001:2013: A.5.1 Management direction for information security, A.6.1 Internal organization, A.18.1.4 Privacy and protection of personally identifable information, A.18.2 Information security reviews

4.2. Incident Response Management

Support for security breach response and data breach process.

Technical Measures

- ✓ Use of firewall and regular updating
- ✓ Use of spam filter and regular updating
- ✓ Use of virus scanner and regular updating
- ✓ Intrusion Detection System (IDS) for customer systems on order
- ✓ Intrusion Prevention System (IPS) for customer systems on order

Organizational Measures

- ✓ Documented procedure for handling security and data protection incidents
- ✓ Documentation of security incidents and data breaches via ticket system

The measures refer to the following controls (Annex A) from IEC/ISO 27001:2013: A.12.2 Protection from malware, A.12.6 Technical vulnerability management, A.13.1 Network security management, A.16.1 Management of information security incidents and improvements, A.18.1.1 Identification of applicable legislation and contractual requirements

4.3. Data Protection by Design and by Default

Measures pursuant to Art 25 GDPR that comply with the principles of data protection by design and by default.

Technical Measures

- ✓ Use of data protection-friendly default settings in standard and individual software

Organizational Measures

- ✓ Documented requirements for "privacy by design / default" are available
- ✓ Requirements for secure software developments are defined

The measures refer to the following controls (Annex A) from IEC/ISO 27001:2013: A.14.1 Security requirements of information systems, A.14.2 Security in development and support processes, A.A.18.2 Information security reviews

4.4. 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

- ✓ Monitoring of remote access by external parties, e.g. in the context of remote support
- ✓ Monitoring of subcontractors according to the principles and with the technologies according to the preceding chapters 1, 2

Organizational Measures

- ✓ Supplier assessments are carried out on a risk basis Documentation of security incidents and data
- ✓ Prior review of the security measures taken by the contractor and their documentation
- ✓ Selection of the contractor on the basis of defined criteria
- ✓ Conclusion of the necessary data processing agreement or EU standard contractual clauses
- ✓ Framework agreement on contractual data processing within the group of companies
- ✓ Regular review of the contractor and its level of protection

The measures refer to the following controls (Annex A) from IEC/ISO 27001:2013: A.13.2 Information transfer, A.15.1 Information security in supplier relationships, A.15.2 Supplier service delivery management, A.18.1.4 Privacy and protection of personally identifable information

5. Certifications

Both the **Quality Management System according to ISO 9001** and the **Information Security Management System according to ISO 27001** of essential parts of Anexia incl. DATSIX data center are **certified** by the independent TÜV NORD CERT GmbH.

Measure	Certified according to ISO 27001 & ISO 9001
Physical Access Control	✓
Logical Access Control	✓
Authorization Control	✓
Transfer Control	✓
Input Control	✓
Order Control	✓
Availability Control	✓
Separation Control	✓
Internal Organization	✓