DPA ANNEX 1

—

TECHNICAL AND ORGANIZATIONAL MEASURES (TOM)

AS OF: November 2023

—

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 (in ANX04)
- ✓ 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
- ✓ Visitor's book / Visitor's protocol
- ✓ Employee / Visitor badges
- ✓ Visitors accompanied by employees
- ✓ Care in selection of security guard personnel
- ✓ Care in selection of cleaning services

1.2. Logical 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

- ✓ Login with username + strong password
- ✓ Anti-Virus Software Servers
- ✓ Anti-Virus-Software Clients
- ✓ Anti-virus software mobile devices
- ✓ Firewalls with Intrusion Detection/Intrusion Prevention Systems (IDS/IPS)
- ✓ 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
- ✓ Access regulations for office locations and data centers

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

- ✓ Central user and authorization management
- ✓ Encryption of data-at-rest and data-in-transit
- ✓ Logging and Monitoring

Organizational Measures

- ✓ Use of authorization concepts
- ✓ Minimum number of administrators
- ✓ Management of user rights by administrators
- ✓ Policy for cryptographic procedures

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

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
- ✓ Policy for cryptographic procedures

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
- ✓ High-availability systems for critical systems

Organizational Measures

- ✓ Existence of an emergency plan
- ✓ Regular maintenance and testing of air conditioning systems, extinguishing systems, batteries, and diesel generators
- ✓ Disaster recovery plans
- ✓ Disaster recovery tests

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

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

4.2. Incident-Response-Management

Support for security breach response and data breach process

Technical Measures

- ✓ Centralized reporting channel for security breaches and data incidents
- ✓ Extensive logging and monitoring for forensic investigations

Organizational Measures

- ✓ Documented procedure for handling security and data protection incidents
- ✓ Documentation of security incidents and data breaches via ticket system
- ✓ Defined roles and responsibilities in the organization
- ✓ Training and sensitization for employees

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

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 based on defined criteria
- ✓ Conclusion of the necessary data processing agreements
- ✓ Framework agreement on contractual data processing within the group of companies
- ✓ Regular review of the contractors and their level of protection

5. Certificates

Both the **Quality Management System according to ISO 9001** and **the Information Security Management System according to ISO 27001** of essential parts of Anexia and DATSIX data center are certified by the independent TÜV NORD CERT GmbH. Additionally, the **Data Protection Management System according to ISO 27701** of essential parts of Anexia as well as DATASIX data center are certified by the independent CIS – Certification & Information Security Services GmbH.