DPA ANNEX 1

—

TECHNICAL AND ORGANISATIONAL MEASURES (TOM)

STATUS: January 2026

—

This document supplements the data processing agreement (DPA) concluded between the client and the contractor pursuant to Art 28 GDPR (EU General Data Protection Regulation).

The technical and organisational measures are implemented by Anexia in accordance with Art 32 GDPR. They are continuously improved by Anexia in line with feasibility and the state of the art – not least in the spirit of the active ISO 27001 certification – and raised to a higher level of security and protection.

1. Confidentiality

1.1. Physical access control

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

Technical measures

- ✓ Alarm system
- ✓ Automatic access control system
- ✓ Biometric access control data centre
- ✓ Chip cards / transponder systems
- ✓ Manual locking system
- ✓ Doors with knob on the outside
- ✓ Doorbell system with camera
- ✓ Video surveillance of entrances

Organisational measures

- ✓ Key regulation / key list
- ✓ Reception / front desk / doorman
- ✓ Visitor book / visitor log
- ✓ Employee / visitor badges
- ✓ Visitors accompanied by employees
- ✓ Careful selection of security personnel
- ✓ Careful selection of cleaning services

1.2. System access control

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

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 in notebooks / tablets / smartphones
- ✓ Two-factor authentication in data centre operations and for critical systems

Organisational measures

- ✓ Management of user permissions according to the need-to-know principle
- ✓ Central creation of user profiles
- ✓ User and password policies
- ✓ Application of security measures for teleworking in accordance with the state of the art
- ✓ Restricted use of administrative user accounts
- ✓ Access regulations for office locations and data centres

1.3. Data access control

Measures ensuring that persons authorised to use a data processing system can access only the data subject to their access authorisation, and that personal data cannot be read, copied, modified or removed without authorisation during processing, use and after storage.

Technical measures

- ✓ Central user and permission management
- ✓ Encryption of data-at-rest and data-in-transit
- ✓ Logging and monitoring

Organisational measures

- ✓ Use of authorisation concepts
- ✓ Minimal number of administrators
- ✓ Management of user rights by administrators
- ✓ Policy for cryptographic procedures

1.4. Separation control

Measures ensuring 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 production and test environments
- ✓ Physical separation (systems / databases / data carriers)
- ✓ Multi-tenancy of relevant applications
- ✓ VLAN segmentation of networks
- ✓ Customer systems logically separated
- ✓ Staging of development, test and production environments

Organisational measures

- ✓ Definition of database rights
- ✓ Defined requirements for development environments
- ✓ Defined requirements for conducting tests in software development

2. Integrity

2.1. Transfer control and input control

Measures ensuring that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or input, during their transport or their storage on data carriers, and that it can be verified and established to which bodies a transfer of personal data by means of data transmission facilities is intended.

Technical measures

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

Organisational measures

- ✓ Implementation of the need-to-know principle
- ✓ Policy for cryptographic procedures

3. Availability and resilience

3.1. Availability control

Measures ensuring that personal data are 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

- ✓ Fire and smoke detection systems
- ✓ Fire extinguishers server room
- ✓ Server room monitoring of temperature and humidity
- ✓ Air-conditioned server room
- ✓ UPS system and emergency power data centre
- ✓ Protective power strips server room
- ✓ RAID system / hard disk mirroring
- ✓ Video surveillance server room
- ✓ Use of protection programs against malware
- ✓ High-availability systems for critical systems

Organisational measures

- ✓ Existing emergency preparedness planning
- ✓ Regular maintenance and testing of air conditioning systems, extinguishing systems, batteries and diesel generators
- ✓ Disaster recovery plans
- ✓ Disaster recovery tests

3.2. Recoverability

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

Technical measures

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

Organisational measures

- ✓ Recovery concept
- ✓ Control of the backup process
- ✓ Regular data recovery tests and logging of the results
- ✓ Storage of backup media in a secure location 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 access for employees
- ✓ Annual review of the adequacy of the TOM

Organisational measures

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

4.2. Incident response management

Support in responding to security breaches as well as data breach process.

Technical measures

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

Organisational measures

- ✓ Documented procedure for handling security and data protection incidents
- ✓ Documentation of security incidents and data breaches via ticket system
- ✓ Defined roles and responsibilities within the organisation
- ✓ Training and awareness-raising for employees

4.3. Privacy-friendly default settings

"Privacy by design" / "privacy by default" pursuant to Art 25 para 2 GDPR.

Technical measures

- ✓ Application of privacy-friendly default settings in standard as well as custom software

Organisational measures

- ✓ Documented requirements for "privacy by design / default" are in place
- ✓ Requirements for secure software development are defined

4.4. Order control (outsourcing, subcontractors and data processing)

Measures ensuring 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 as per the preceding chapters 1, 2

Organisational measures

- ✓ Supplier assessments are carried out on a risk basis
- ✓ 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 agreement
- ✓ Framework agreement on data processing within the group of companies
- ✓ Regular review of the contractor and its level of protection

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 as well as the DATASIX data centre operations** are **certified** by the independent TÜV NORD CERT GmbH. In addition, the **data protection management system according to ISO 27701** of essential parts of **Anexia as well as the DATASIX data centre operations** is certified by the independent CIS - Certification & Information Security Services GmbH.