DPA ANNEX 1

—

TECHNICAL AND ORGANIZATIONAL MEASURES (TOM)

AS OF: SEPTEMBER 2020

—

The present document supplements chapter 11 of 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 DSGVO. 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
- ✓ Biometric access control data center

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
- ✓ Information Security Policy
- ✓ Work instructions for operational safety
- ✓ Work instruction access control

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
- ✓ Intrusion Detection Systems
- ✓ Use of VPN for remote access
- ✓ Encryption of data carriers
- ✓ Encryption of smartphones
- ✓ Automatic desktop lock
- ✓ Encryption of notebooks / tablet
- ✓ Two-factor authentication in data center operation and for critical systems

Organizational Measures

- ✓ User permission management
- ✓ Creating user profiles
- ✓ Central password assignment
- ✓ Information Security Policy
- ✓ Work instruction IT user regulations
- ✓ Work instruction operational security
- ✓ Work instruction access control
- ✓ Mobile Device Policy

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
- ✓ Logging of accesses to applications, specifically when entering, changing, and deleting data
- ✓ SSH encrypted access
- ✓ Certified SSL encryption

Organizational Measures

- ✓ Use of authorization concepts
- ✓ Minimum number of administrators
- ✓ Management of user rights by administrators
- ✓ Information Security Policy
- ✓ Work instruction communication security
- ✓ Work instruction Handling of information and values

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
- ✓ Client systems logically separated
- ✓ Staging of development, test and production environment

Organizational Measures

- ✓ Control via authorization concept
- ✓ Determination of database rights
- ✓ Information Security Policy
- ✓ Data Protection Policy
- ✓ Work instruction operational security
- ✓ Work instruction security in software development

1.5. Pseudonymization

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures.

Technical Measures

- ✓ In case of pseudonymization: separation of the allocation data and storage in separate system (encrypted)
- ✓ log files are pseudonymized at the request of the client

Organizational Measures

- ✓ Internal instruction to anonymize/pseudonymize personal data as far as possible in the event of disclosure or even after the statutory deletion period has expired
- ✓ Information Security Policy
- ✓ Data Protection Policy
- ✓ Specific internal regulations on cryptography

2. Integrity

2.1. Transfer Control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission 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 and secure cloudstores
- ✓ Use of signature procedures (case-dependent)

Organizational Measures

- ✓ Survey of regular retrieval and transmission processes
- ✓ Transmission in anonymized or pseudonymized form
- ✓ Careful selection of transport personnel and vehicles
- ✓ Personal handover with protocol
- ✓ Information Security Policy
- ✓ Data Protection Policy

2.2. Input Control

Measures that ensure that it is possible to check and establish retrospectively whether and by whom personal data has been entered into, modified or removed from data processing systems. Input control is achieved through logging, which can take place at various levels (e.g., operating system, network, firewall, database, application).

Technical Measures

- ✓ Technical logging of the entry, modification and deletion of data
- ✓ Manual or automated control of the logs (according to strict internal specifications)

Organizational Measures

- ✓ Survey of which programs can be used to enter, change or delete which data
- ✓ Traceability of data entry, modification and deletion through individual user names (not user groups)
- ✓ Assignment of rights to enter, change and delete data on the basis of an authorization concept
- ✓ Retention of forms from which data has been transferred to automated processes
- ✓ Clear responsibilities for deletions
- ✓ Information Security Policy
- ✓ Work instruction IT user regulations

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
- ✓ Protective socket strips server room
- ✓ RAID system / hard disk mirroring
- ✓ Video surveillance server room
- ✓ Alarm message in case of unauthorized access to server room

Organizational Measures

- ✓ Backup concept
- ✓ No sanitary connections in the server room
- ✓ Existence of an emergency plan
- ✓ Storage of backup media in a secure location outside the server room
- ✓ Separate partitions for operating systems and data where necessary
- ✓ Information Security Policy
- ✓ Work instruction operational security
- ✓ Regular testing of the diesel aggregates

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
- ✓ Existence of an emergency plan
- ✓ Information Security Policy
- ✓ Work instruction operational security

4. Procedures for regular Review, Assessment and Evaluation

4.1. Data Protection Management

Technical Measures

- ✓ Central documentation of all data protection regulations with access for employees
- ✓ Security certification according to ISO 27001
- ✓ A review of the effectiveness of the TOMs is carried out at least annually and TOMs are updated
- ✓ Data protection checkpoints consistently implemented in tool-supported risk assessment

Organizational Measures

- ✓ Internal data protection officer appointed: Group Data Protection Officer, DPO
- ✓ Staff trained and obliged to confidentiality/data secrecy
- ✓ Regular awareness trainings at least annually
- ✓ Internal Information Security Officer appointed: Group Information Security Officer, ISO
- ✓ Data Protection Impact Assessment (DPIA) is carried out as required
- ✓ Processes regarding information obligations according to Art 13 and 14 GDPR established
- ✓ Formalized process for requests for information from data subjects is in place
- ✓ Data protection aspects established as part of corporate risk management
- ✓ ISO 27001 certification of key parts of the company including data center operations and annual monitoring audits

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 process for detecting and reporting security incidents / data breaches (also with regard to reporting obligation to supervisory authority)
- ✓ Formalized procedure for handling security incidents
- ✓ Involvement of DPO and ISO in security incidents and data breaches
- ✓ Documentation of security incidents and data breaches via ticket system
- ✓ A formal process for following up on security incidents and data breaches
- ✓ Information Security Policy
- ✓ Data Protection Policy
- ✓ Work instruction oprational security
- ✓ Work instruction IT user regulations

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

- ✓ No more personal data is collected than is necessary for the respective purpose
- ✓ Use of data protection-friendly default settings in standard and individual software

Organizational Measures

- ✓ Data Protection Policy (includes principles "privacy by design / by default")
- ✓ OWASP Secure Mobile Development Security Checks are performed
- ✓ Perimeter analysis for web applications

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

- ✓ Work instruction supplier management and supplier evaluation
- ✓ Prior review of the security measures taken by the contractor and their documentation
- ✓ Selection of the contractor under due diligence aspects (especially with regard to data protection and data security)
- ✓ Conclusion of the necessary data processing agreement on commissioned processing or EU standard contractual clauses
- ✓ Framework agreement on contractual data processing within the group of companies
- ✓ Written instructions to the contractor
- ✓ Obligation of the contractor's employees to maintain data secrecy
- ✓ Agreement on effective control rights over the contractor
- ✓ Regulation on the use of further subcontractors
- ✓ Ensuring the destruction of data after termination of the contract
- ✓ In the case of longer collaboration: ongoing review of the contractor and its level of protection

5. Organization and Data Protection at Anexia

In its strategic guideline Quality, Risk and Compliance Policy, the Anexia Group of Companies has set itself the goal, among other things, of providing its customers with the products and services to be delivered at the highest possible level of information security in compliance with the law. This guideline provides the framework for transparent, sustainable, process-based and risk-oriented management of the corporate group within the framework of an Integrated Management System (IMS).

In this context, Anexia has established a distinctive cross-sectional security organization to ensure comprehensive protection of its own corporate information and data as well as protection of the data of its customers and clients. The functions of Information Security Officer (ISO), Data Protection Officer (DPO), Quality Officer (QO), Risk Officer (RO) and Legal Compliance Officer (LCO) with group-wide responsibility and direct authority in these areas of activity have been established within the staff department "Quality, Risk & Compliance", which is directly assigned to the CEO, and a comprehensive set of internal guidelines and regulations ("Anexia Corporate Binding Rules" on information security and data protection, among other things) has been established, which is binding for all employees and defines secure and data protection-compliant handling of information and data.

Employees are continuously informed and trained in the area of data protection. In addition, all employees are contractually bound to data secrecy and confidentiality. External parties who may come into contact with personal data in the course of their work for Anexia are obligated to maintain secrecy and confidentiality as well as to comply with data protection and data secrecy by means of a so-called NDA (Non-Disclosure Agreement) before they begin their work.

All affiliated companies of the Anexia group of companies within the EU or the EEA have concluded a joint framework agreement on data protection and commissioned data processing as a binding written legal instrument pursuant to Art 28 GDPR in order to ensure a uniformly high standard of data protection and data security across the entire group and to clearly regulate the rights and obligations for any commissioned data processing.

Any subcontractors entrusted with further processing (as “other processors”) are only used after approval by the Client as the “controller” and after conclusion of a Data Processing Agreement (DPA) in accordance with Art 28 GDPR, with which they are fully bound by all data protection obligations to which Anexia itself is subject.

All of these organizational measures are flanked by Anexia's current, high technical security standards, and both dimensions are periodically reviewed and confirmed for adequacy and effectiveness in the course of ongoing internal audits and annually by independent, external, DAkkS-accredited certification bodies as part of the ISO 9001 and ISO 27001 monitoring and re-certification audits.

6. 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. data center operation are certified by the independent TÜV NORD CERT GmbH.

Measures overview:

Measure	GDPR compliant implemented	Comments
Physical Access Control	✓	ISO 27001 & ISO 9001 certified
Logical Access Control	✓	ISO 27001 & ISO 9001 certified
Authorization Control	✓	ISO 27001 & ISO 9001 certified
Separation Control	✓	ISO 27001 & ISO 9001 certified
Pseudonymization	✓	ISO 27001 & ISO 9001 certified
Transfer Control	✓	ISO 27001 & ISO 9001 certified
Input Control	✓	ISO 27001 & ISO 9001 certified
Availability Control	✓	ISO 27001 & ISO 9001 certified
Recoverability Control	✓	ISO 27001 & ISO 9001 certified
Data Protection Management	✓	ISO 27001 & ISO 9001 certified
Incident Response Management	✓	ISO 27001 & ISO 9001 certified
Privacy by Design and by Default	✓	ISO 27001 & ISO 9001 certified
Order Control	✓	ISO 27001 & ISO 9001 certified
Organization	✓	ISO 27001 & ISO 9001 certified