Introduction DPA ANNEX 1

Technical and Organizational Measures (TOM)

As of January 2023

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 Outpost24 in accordance with Art 32 DSGVO. They are continuously improved by Outpost24 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.

Document Control

Document prepared by Eren Cihangir, Product Expert
Document approved by Martin Jartelius, CISO, January 17th 2023
Version 1.0

Data Processing

Information about the processor

- Processing takes place at the processor
- Mobile end devices are used for processing (laptops)
- Data processing can take place within home office or remote activity
- The service is a SaaS application hosted by the processor or a sub-processor

Pseudonymisation and Encryption, Art. 32 (1)(a) GDPR

Pseudonymisation

- The solutions rely on user identification via email and username, customers can set this in a way where it's not discernible to processor who the holder of an identity is, if they prefer to.

Encryption

- All data in transit with the solution is encrypted using strong cryptography in good standing
- All remote access is encrypted and requiring unique identification
- VPN-connection (IP-Sec) [needed for remote access]

- Email encryption is employed if data is transferred via email – this is applicable only to the services organisation as no data is transferred related to other customers
- Data transfer with https-connection
- Full disc encryption of laptop hard drives
- Full disc and content encryption of other mobile devices used to access corporate email

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

- Keys
- Electronic access code cards/access transponders
- Locking of data processing equipment (e.g., locked cage for server)
- Other: Personal codes, personal smart-keys, physical keys with digital certificates with remote revocation for access to data processing facilities

Physical Measures

- Burglary alarm system/alarm system
- Video surveillance
- Separately secured, locked access to server rooms
- Regular inspection and maintenance of the above systems

Organizational Measures

- Key regulations
- Instructions on the issue of keys
- Graded security areas and controlled physical access
- Physical access authorisation concept:
    - Authorisation IDs
    - Visitor IDs, visibly carried or escorted by own employees
    - Presence recordings of visitor accesses
- Locking doors and windows also during office hours
- Data media stored locked or in locked rooms with access control
- Security also outside working hours, via security firm
- Third party auditing concerning service providers and third parties (e.g., cleaning and maintenance services) staff and background checks

Electronic Access Control

The organization employ a range of technical controls, from logging and monitoring to user behaviour analytics. The most asked for are listed below, but those controls are changing and consistently enhanced.

Technical Measures

- Password protection of computer workstations
- Automatic password-protected lock screen after inactivity
- 2-minute period of inactivity
- Functional and/or time-limited assignment of user authorisations
- Use of individual passwords, even initial ones
- Automatic blocking of user accounts
- Time delay for retries after 3 incorrect password entries
- Hashing of stored passwords
- Two-factor authentication
- Password policy tied to NIST password guidelines
- Password changes:
    - The reuse of already used passwords is suppressed (password history)
    - 12 Generations of password history
- Monitoring for logins deviating from norm
    - New devices with failed pass
    - New devices with good pass but failed MFA
    - Impossible travel detection
    - Uncommon location for user alerting
    - Uncommon access behaviour for system resources

Organizational Measures

- Regulated process for granting rights for new employees joining the company
- Regulated process for withdrawing rights when tasks of employees change
- Regulated process for withdrawing rights of employees leaving the company
- Confidentiality obligation
    - Employees
    - Third parties/ processors
- Logging and evaluation of system usage
- Role based access – no individual access is assigned, all are tied to a role description and responsibility in the identity provider source

Physical Measures

- Visual protection of computer workstations and laptops used in a mobile way
- Privacy screens

Internal Access Control

Technical measures

- Determination of access authorisations, authorisation concept
- Regular review of access authorisations
- Minimal access for roles applied
- Logging of system access
- Logging of file access
- Usage of appropriate security systems (software/hardware)
    - Virus scanner
    - Firewalls
    - SPAM filter
    - Intrusion prevention (IPS)
    - Intrusion detection (IDS)
    - Software for Security Information and Event Management (SIEM)
- Restricted and logged database access
- Regular evaluation of logs
- Regular review of privileged activities

Separation Control

Organizational measures

- ✓ Logical separation of customers
- ✓ Authorisation concept that takes account of the separate processing of data from different clients
- ✓ Separation of functions
- ✓ Separation of development, test, and deployment systems
- ✓ Logical data separation
- ✓ Processing of data of the controller and data of other customers by different employees of the processor
- ✓ Guidelines and work instructions for employees
- ✓ Implemented clear desk policy
- ✓ Regulation for restoring data from backups
- ✓ Development and operations separated
- ✓ Release controls with separation
- ✓ Privileged access requests by senior analysts managed by independent team in operations

Transfer Control

Transfer Media

- ✓ File transfers always using encryption
- ✓ GPG for sensitive email
- ✓ HTTPS for portal access
- ✓ Secure file transfer using OUTSCAN
- ✓ Bitwarden encrypted single use file-transfer

Data Transfer

- ✓ General regulation for data transmission
- ✓ Documented administration of data media, inventory control
- ✓ Determination of the areas where data media must be kept
- ✓ Data media disposal–secure destruction of data media:
  - Destruction according to DIN 66399
- ✓ Shredding capabilities at all facilities processing information on paper (paper copies not allowed for sub processing of data)
- ✓ Packaging and shipping rules
- ✓ Encrypted e-mail transfer via:
  - End-to-end encryption
  - Transport encryption

Data entry control

- ✓ Labelling of collected data
- ✓ Determination of user authorisations
- ✓ Differentiated user authorisations:
  - Read, write, delete [erase]
  - Partial access to data or functions
  - Field access in databases
- ✓ Organisational determination of data entry responsibilities
- ✓ Logging of entries/erasures
- ✓ Regulation on storage periods for the purpose of audit/evidence purposes
- ✓ Regulation of access authorisation for log servers (log admin)
- ✓ Log concept exceeding OS standard
- ✓ Dedicated log servers

Availability and Resilience, Art. 32 (1)(b) GDPR

Resilience control

Physical measures

- Fire protection
- Smoke detectors in server rooms
- Fire alarm systems in server rooms
- Waterless firefighting systems in server rooms
- Server rooms in a separate fire compartment
- Placement of backup systems in separate rooms and fire compartments
- Redundant Power supply
- UPS (Uninterruptible Power Supply) system (uninterruptible power supply)
- Emergency power system
- Functionality protection
- Lightning/overvoltage protection
- Air-conditioned server rooms
- Water sensors in server rooms
- Protection of the servers against firefighting water

Data security and backup concepts

- Cloud Backup in encrypted format stored with key not present
- Backup located in a separate data centre
- Several backup iterations
- Backup system cannot overwrite prior backups
- Automated retention by age and retention policy
- Restore tests performed regularly of backups
- Existing recovery concept

Organisational measures

- Restricted access to server rooms for authorized personnel only
- Inventory and documentation of IT systems and applications
- Disaster or emergency plans (e.g., water, fire, explosion, loss of data centre)
- Weak spot and vulnerabilities analysis (site protection, building protection, penetration into computers, computer networks)
- Consideration of the impact of neighbouring buildings and structures

Resiliency measures

- Substitute data centres or another backup system available (hot standby systems, restorable fail over site)
- Redundant power supply
- Redundant uninterruptible power supply (UPS) system
- Redundant air conditioning
- Data storage on RAID systems (RAID 1 and higher)
- Performance of penetration tests
- Performance of vulnerability scanning and management
- System hardening (deactivation of unnecessary services and components)
- Prompt and regular activation of available software and firmware updates
- Periodic training and awareness campaigns within the organisation

- Inventory of IT devices, assets, and network systems in the organisation's infrastructure
- Planned maintenance of systems
- Capacity measurement and management
- Security of cabling (data cable/power cable/telecommunications cable)

Restorability, Art. 32 (1)(c) GDPR

Rapid recovery

- Current data backup
- Documentation of the systems
- Regular restore tests

Procedures for regular testing, assessment and evaluation of technical and organisational measures, Art. 32 (1)(d) GDPR, Art. 25 (1) GDPR

Data protection management

Organizational measures

- Regular internal controls of security measures
- Responsibilities for data protection and information security are defined
- ISO27001 certified ISMS
- The management team is regularly informed about the status of data protection, information security and possible risks and consequences due to missing measures.
- If the aforementioned review is negative, the security measures are adapted, renewed, and implemented on a risk-related basis.
- Circumstances of permitted private use of corporate assets are regulated
- Prohibited corporate use of private devices (BYOD) for data processing
- Permitted handling and use of data media regulated
- Personal data is categorized according to risk

Incident response process

- ✓ Message path for events and weaknesses ensured
- ✓ Evaluation of security breaches and system malfunctions
- ✓ Plans for dealing with detected attacks and malfunctions
- ✓ Documentation and evaluation of evidence
- ✓ Retained registration and follow up on all incidents

Data protection by design and default

- By implementing the technical and organisational measures, the processor enables the controller to comply with the principles of Art. 5 (1) GDPR, in particular:
  - Data minimisation
  - Purpose limitation
  - Storage limitation
- Pre-setting of data protection-friendly settings where applicable.

Order or contract control

- Contract drafting according to legal requirements (Art. 28 GDPR)
- Recording of existing sub-processors
- Reviews and inspections of sub-processors
- On-site inspections of sub-processors for critical sub-processors
- Review of the sub-processor's data protection concept
- Inspection of the sub-processor's existing IT security certificates
- Strict controls on the selection process