

Appendix 5: Data Protection and Order Processing

This document provides an overview of data protection and the basic principles of order processing in accordance with Article 28 of the General Data Protection Regulation (“GDPR”), which have been implemented for the operation of the transparency platform.

Basic Architecture of the Platform

The transparency platform consists of the following components:

1. Application server for storing data and processing queries
2. TR tool for sending report data and report queries
3. Web service for receiving and archiving report data and report queries
4. Public key infrastructure (PKI) for issuing and managing security certificates

These components cater for high availability and meet all the current requirements for fail-safe operation.

By utilising a zone concept, current, standard mechanisms for ensuring a consistent, high level of security are in place.

Data Integrity (Integrity)

Encryption mechanisms are implemented to ensure the integrity of report data. In particular,

- reporting data,
- reporting queries,
- and response data

are stored on the platform with encryption. In addition, all messages receive a timestamp so that changes to messages can be monitored. Furthermore, unauthorised changes to content cannot be made because messages require a signature.

Current "state-of-the-art" encryption methods are used to encrypt messages.

Confidentiality

Special attention is paid to the confidentiality of data on the transparency platform.

The EEX receives data on behalf of Seven2one, the technical operator of the platform, and processes it in accordance with Article 28 of the General Data Protection Regulation (“GDPR”). In this context, the EEX can access and process personal data in order to perform the agreed services.

Nature and Purpose of Processing, Type of Data and Categories of Data Subjects

The data are stored, queried, and reused.

The purpose of processing is defined in the data provision contract.

The following types of personal data are processed by EEX:

- First name, surname, title
- Professional contact data
- Contract master data (contractual relationship, product/contractual interest)
- Billing and payment data

Data from the reporting company are affected.

Locations of Data Processing

The processing and use of client data take place exclusively in a Member State of the European Union. If data are transferred to a third country that does not offer an adequate level of protection, additional guarantees must be in place in accordance with Article 44 et seqq. GDPR.

Rectification, Blocking, and Erasure of Data

Data shall only be corrected, deleted, or blocked upon submission of a documented instruction by the reporting company.

A. Data Security Concept according to Art. 32 GDPR - EEX

1. Confidentiality according to (Art. 32 para. 1 lit. b GDPR)

1.1 Measures to protect against unauthorised physical access

- Company grounds and buildings are monitored using video surveillance, security patrols, break-in sensors, and other technical and organisational monitoring measures.
- ID checks by gatekeepers.
- Only authorised persons are permitted to gain entry after their identity has been checked and confirmed.
- Access authorisation is granted based on relevant authorisation procedures.

1.2 Measures for logical access control

- Users can protect sessions using screen savers and accompanying passwords. Sessions can be temporarily locked.

Further measures are defined by Seven2one and Microsoft on a system basis; at the same time, Seven2one also operates the system in which commissioned data processing takes place.

B. Data Security Concept according to Art. 32 GDPR – Seven2one

1. Confidentiality (Art. 32 para. 1 lit. B GDPR)

1.1 Physical access control

- Technical or organisational measures for access control, particularly for legitimising authorised persons:
 - Access control systems on the contractor's premises:
 - Security locking system in office space with documented assignment of keys
 - Server room also secured with locking system, assignment of keys documented
 - Alarm system for office floors
 - Access control systems for external premises (in data centre):

- Max. Utilisation of data centre-specific measures (security locking system, alarm system, access control/documentation)

1.2 System access control

Technical (password/password protection) and organisational (user master record) measures regarding user identification and authentication:

- Password policy (active directory):
 - Passwords must be changed every 180 days
 - Passwords must be at least 8 characters long
 - Passwords must meet a standard of password complexity (3 out of 4)
 - Automatically blocked after 6 invalid attempts, manual reset
- One user master record setup per user (personal accounts)
- Dial-up via VPN only possible from contractor computers and only after activation, encryption via SSL-VPN
- Firewall
- Virus protection

1.3 Data access control

Requirements-oriented design of the authorisation concept and access rights as well as their monitoring and logging:

- Differentiated authorisations (roles, groups, objects, and profiles)
 - Read
 - Change
 - Delete
- Email contact details via encrypted connection
- Remote access only via encrypted VPN connection or via authorised TeamViewer access: access details for remote access to the customer system are stored securely (e.g., in a password safe); delivery or access granted by support and consulting employees on a need-to-know basis (i.e., only for those employees who need access for their work).

1.4 Separation control

Measures for the separate processing (storage, modification, deletion, transmission) of data with different purposes:

- Separate storage of data of different customers
- Single purpose of data processing as part of software maintenance
- Separation of functions by department/order in other cases
 - Support -> test
 - Development -> test, error correction, new development
 - Consulting -> test, adjustments, error correction
 - QA -> error correction, test

1.5 Pseudonymisation

Particularly irrelevant in remote maintenance; data are provided by the client in a pseudonymous form unless personal reference is required to execute the job (e.g., test purposes).

2. Integrity (Art. 32 para. 1 lit. b GDPR)

2.1 Transfer control

Measures taken during the transport, transfer/transmission, or storage of data on data carriers (manually or electronically), plus subsequent reviews:

- WebDav (encryption via SSL)
- USB sticks are encrypted
- Remote access only via encrypted VPN connection
- In principle, customer data should not be stored locally on notebooks and/or mobile data carriers belonging to employees of the contractor (if local storage is required on a particular occasion or if the client requests this, then only encrypted notebooks shall be provided for this purpose).

2.2 Input control

The client is responsible for subsequent checks regarding whether and by whom data was entered, changed, or removed (deleted):

- Logging options available (storing changes in master data, order data, etc.,)

3. Availability and Resilience (Art. 28 para. 1 lit. b GDPR)

3.1 Availability control

Measures for backing up data (physical/logical) on the side of and locally at the contractor (does not release the client from their obligation to back up data in their own area of responsibility):

- Mirroring of hard drives, RAID level
- Uninterruptible power supply (UPS)
- Virus protection/firewall
- Cloning systems to other storage areas
- Air conditioning
- Emergency plan

4. Procedure for regular checks, assessment, and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

4.1 Data protection management

The contractor's employees shall comply with the requirements contained in the General Data Protection Regulation; binding rules of conduct apply. The contractor has a data protection officer and documented data processing processes.

4.2 Order control

The client is responsible for order control.

C. Data Security Concept according to Art. 32 GDPR – Microsoft

Microsoft has taken the following security measures for customer data in the core online services, and shall retain these measures, which, in connection with the security obligations in the OST, represent the individual responsibility of Microsoft in relation to the security of these data.

1. Organisation of information security

Responsibility for security. Microsoft has appointed one or more security representatives who are responsible for the coordination and monitoring of the security provisions and procedures.

Roles and responsibilities in relation to security. Employees of Microsoft with access to customer data are subject to confidentiality obligations.

Risk management programme. Microsoft has carried out a risk assessment before the processing of customer data or the introduction of the service for online services.

Microsoft stores its security documents in accordance with their storage requirements after they are no longer valid.

2. Inventory management

Inventory creation. Microsoft maintains a stock inventory of all media in which customer data are stored. Access to the stocks of this media is reserved for Microsoft employees who have been authorised in writing to have this access.

Handling of stock

- Microsoft splits customer data into categories in order to make identification easier and enable an appropriate restriction of access to customer data.
- Microsoft imposes restrictions for the printing of customer data and has procedures for the disposal of printed materials that contain customer data.

- Microsoft staff must receive permission from Microsoft before they store customer data on portable devices, access customer data remotely, or process customer data outside the facilities of Microsoft.

3. Security in human resources

Security training. Microsoft informs its employees about relevant security procedures and their respective tasks. Microsoft also informs its employees about possible consequences of violations of the security provisions and procedures. Microsoft only uses anonymous data in training.

4. Physical security and security of the environment

Physical access to facilities. Microsoft restricts access to facilities, in which its information systems that process customer data are located, to named authorised personnel.

Physical access to components. Microsoft keeps documents about the incoming and outgoing media that contain customer data, including the type of media, authorised senders/recipients, date and time, quantity of the media, and the type of customer data they contain.

Protection against disruptions. Microsoft uses different systems according to the industry standard to prevent the loss of data due to power outages or line failures.

Disposal of components. Microsoft uses procedures according to the industry standard to delete customer data when they are no longer needed.

5. Communication and operations management

Operative guideline. Microsoft keeps security documents in which the security measures and the relevant processes and responsibilities of its employees, who have access to customer data, are described.

Data recovery process

- Microsoft creates multiple current copies of customer data that can be reproduced, on an ongoing basis but no less than once per week in any case (unless no customer data are updated in that time period), and stores them.
- Microsoft keeps copies of customer data and data recovery processes at a different location to the place in which the primary computer devices that process the customer data are located.
- Microsoft has certain processes that regulate access to copies of customer data.
- Microsoft reviews the data recovery process at least every six months, with the exception of the process for Azure services for administration, which are reviewed every twelve months.

- Microsoft logs data recovery measures, including the person responsible and the description of the recovered data; if necessary, the person responsible and which data (if necessary) must be entered manually during the data recovery process.

Malware. Microsoft has anti-malware controls in order to prevent malware from receiving unauthorised access to customer data, including malware from public networks.

Cross-border data.

- Microsoft encrypts customer data that are transferred via public networks or enables customers to do so.
- Microsoft restricts access to customer data in media that leave its facilities.

Event logging. Microsoft records access to and the use of information systems that contain customer data by registering the access ID, access time, granted or denied authorisation, and corresponding activity, or enables the customer to do so.

6. Data access control

Access guideline. Microsoft keeps documents about the security authorisations of individual people who access customer data.

Access authorisation

- Microsoft keeps and updates documents about the employees who are authorised to access Microsoft systems that contain customer data.
- Microsoft deactivates login details that have not been used for a period of time that may not exceed six months.
- Microsoft names the employees who are entitled to grant, change, or revoke authorised access to data and resources.
- If multiple people have access to the systems in which customer data are contained, Microsoft ensures that these people have separate identifications/login details.

Minimal authorisation

- Technical support staff are only allowed to access customer data when this is necessary.
- Microsoft restricts access to customer data to only those individuals who need this access to carry out their professional activity.

Integrity and confidentiality

- Microsoft instructs its employees to deactivate administration sessions when they leave facilities under the control of Microsoft or when computers are otherwise left unattended.
- Microsoft stores passwords in such a way that they are not legible during the time of validity.

Authentication

- Microsoft uses processes according to the industry standard to identify and authenticate users who attempt to access information systems.
- If the authentication processes are based on passwords, Microsoft stipulates that the passwords must be replaced regularly.
- If the authentication processes are based on passwords, Microsoft stipulates that passwords must contain at least eight characters.
- Microsoft ensures that deactivated or expired identifications are not issued to any other people.
- Microsoft monitors repeated attempts to establish access to the information systems with invalid passwords, or it enables the customers to do so.
- Microsoft has processes according to the industry standard to deactivate passwords that are corrupted or mistakenly disclosed.
- Microsoft uses processes according to the industry standard to protect passwords, including processes that are intended to safeguard the confidentiality and integrity of passwords, if they are allocated and distributed, and during storage.

Network design. Microsoft has controls to prevent people, who accept access rights that have not been allocated to them, from gaining access to customer data without being authorised to do so.