Data security concept of Omikron Data Quality GmbH (V5.3)

Technical and organizational measures (TOM)

1. Introduction

This documentation provides an overview of the technical organizational measures in place at Omikron Data Quality GmbH (hereinafter referred to as “Omikron” for order processing. The IT systems for all connected offices are located at the headquarters in 75172 Pforzheim.

In 2023, the infrastructure underwent only minor changes, meaning that the documentation of technical and organizational measures hardly needed to be adapted. Restructuring and the creation of new processes had already been successfully implemented and completed in the previous year.

Data protection agreements and corresponding technical and organizational measures are in place for subcontractors and partner companies that offer and distribute Omikron services and products at locations outside Germany.

2. Technical-organizational measures

2.1 Physical access control

Physical access control denies unauthorized persons access to data processing systems with which the data is collected, processed and used.

The doors to Omikron's business premises are equipped with security locks, rigid doorknobs and an automatic puller. Access to the business premises is handled by an electronic access system in Pforzheim.

The doors are also locked during the day and can only be opened using a key or the electronic access system. Furthermore, in the main building the doors are locked outside working hours (22:00 to 06:00) and the premises are secured with an alarm system.

The premises where personal data is processed are secured by a permanently locked door and an access check via RFID chips.

Keys are only issued to authorized persons and permanent employees and are withdrawn as soon as the authorization expires. The same regulation applies to registration for the finger scan.

Windows in the basement are secured with grids against unauthorized entry. The windows on the ground floor, 1st and 2nd floor, are firmly locked outside working hours.

Access to the server room is always locked and is only possible by the IT department and, in an emergency, by the administration.

The building is secured by means of alarm systems.

There is an approved process for granting access and accompanying visitors in the building.

2.2 Data access control

Access control prevents data processing systems from being used by unauthorized persons.

Each authorized person receives an individual user ID and a personal password that must be kept secret and may not be passed on to third parties.

According to the BSI recommendation from February 2020, the regular obligation to change passwords no longer applies.

The password is immediately blocked if authorization expires. Password policies are defined for password complexity and are regularly checked against the recommendations of the BSI.

The password will be blocked immediately if the authorization expires. The password consists of at least 8 characters, where the characters must be randomly selected upper case letters, lower case letters and numbers.

The password conventions shown are (technically) enforced by system settings. Furthermore, there are corresponding password guidelines (organizational).

The workstations are automatically locked after 15 minutes of inactivity. A work instruction to the employees specifies bindingly that the workstation is immediately locked when it is left.

Depending on the system used, the user ID is blocked after a specified number of failed attempts.

Externally accessible, security-relevant systems are secured via multi-factor instances.

Internal networks are protected internally and externally by state-of-the-art firewall systems.

Setting up and blocking access authorizations in the system are documented.

2.3 Access control

Access control restricts the use of a data processing system by authorized persons exclusively to the data subject to their access authorization.

Within the access authorization concept, graded access authorizations are in place that only allow and otherwise prevent the entry, reading, copying, modification or removal of data during processing, use and after storage to the extent required for the respective task.

The permissions at file system level are categorized by corresponding user groups. Task data is stored in specially protected paths on the server and processed there.

Access rights are managed exclusively by the system administrators. The employees involved in the collection, processing and use of data do not have administrator rights on the server.

Data carriers are kept in a locked area after the data has been read in and verified or, if possible, physically destroyed (e.g. CDs, USB flash drives, hard drives).

Administrative activities are restricted to a small group of administrators.

Where possible, general group users that were used by multiple people were replaced with personalized accounts. This also applies to administrative accounts.

2.4 Transfer control

The transfer control prevents unauthorized reading, copying, modification or removal of data during electronic transmission or during transport or when it is stored on data carriers and logs the points at which the transmission of data by data transmission equipment is intended.

The data is transmitted in encrypted form in consultation with the client, taking into account current technologies such as https, VPN and dedicated encryption.

The data recipients and the transport/transmission route are documented.

Furthermore, there are special packaging and shipping regulations for commissioning reliable transport companies with appropriately documented shipping routes.

We have also taken the following measures with regard to the transfer of personal data

- Secure installation of servers and SAN (security area)/NAS
- Company-owned domain for email communication (internal)
- Restriction of the group of persons authorised to transmit data
- Transfer to third parties only after checking the legal basis
- Written specification of the transfer to third countries

2.5 Input control

The input control logs whether and by whom data is entered into data processing systems and changed or removed.

The input control (unauthorized modification, deletion and logging of changes) is implemented by Omikron as follows due to the type of processing (partially automated batch processing):

- All personal data is provided with a unique key before work begins, which uniquely identifies each data record throughout all processing steps up to the final result.
- Before each processing step, the data is stored as a copy for documentation purposes, so that all changes in a processing step can be traced in a dedicated manner. The copies are kept in the same customized work directory tree as the originals. They are deleted with the originals at the end of the assignment.

2.6 Order control

Ensures that personal data processed on behalf of the client are only processed in accordance with the client's instructions.

The basis for the processing of the data is the written commissioning by the client. Omikron will adhere to the latest valid version of the specification for order processing.

Changes requested by the client in the order process will be documented and made available to the client in writing.

Any changes to the order volume and price will be offered separately. The aim of order control within the meaning of Art. 28 EU GDPR is to ensure that personal data processed on behalf of the client can only be processed in accordance with the order and the client's instructions. This is done in accordance with the following aspects:

- Contractual regulation (data processing agreements, DPAs)
- Subcontracting only with an equivalent level of protection
- Review and documentation of measures taken by the contractor
- Obligation of the contractor's employees to maintain data confidentiality

2.7 Availability control

An availability control secures the data against accidental destruction or loss.

Software protection is guaranteed by memory-resident scanners against the violation of system integrity with viruses, Trojans, worms and other malware. The scanner is updated daily (several times if necessary) and provided with new updates.

The operating system and the existing operating and security software are kept up to date with centrally distributed updates and patches.

A spam filter additionally ensures the removal of harmful messages.

An uninterruptible power supply ensures sufficient hardware protection of the server systems on which the data is stored.

The server rooms are operated at an optimal temperature range using air conditioning in order to achieve the highest possible longevity and reliability of the components.

Smoke and fire alarms are in place in accordance with fire safety regulations.

The data backup concept provides for daily backup copies of the data stock, with several backup versions available. In addition, restore attempts are carried out regularly to ensure the possibility of restoring the data.

Depending on the backup measure, deletion takes place on a rolling basis, i.e. by overwriting the old backup copy of the data at the respective backup frequency (daily backups are currently overwritten after 31 days, monthly rolling backups after 12 months).

The backup copies are stored separately on dedicated NAS systems. For important core systems, a tape backup is performed weekly, which is additionally stored securely in a safe deposit box at another location on a monthly basis.

An emergency manual/emergency plan is available.

2.8 Separation control

Separation control ensures that data collected for different purposes can be processed separately.

Data is processed separately for each contractor and project. All data is stored in separate databases and project folders.

The accompanying order documentation serves to document the purposes for which the respective data is to be processed and used.

Order data is accessible to Omikron's own administration for the purpose of data backup and to the employees of the Professional Services department for the purpose of processing.

2.9 Pseudonymization

Pseudonymization means processing 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 this additional information is kept separately and is subject to appropriate technical and organizational measures:

- Pseudonymization using a unique identification number (ID). This ID is used in the system when creating logs and is used, for example, for error checking in databases.
- In addition, the data is anonymized if statistical evaluations are carried out and it is therefore no longer necessary to refer back to the collected data at any point.

2.10 Data privacy

All employees who process or have access to personal or other commissioned data have been committed in writing to data secrecy.

The transfer of or access to personal data to subcontractors will only take place once they have signed a commissioned processing agreement in accordance with Article 28 DS-GVO.