

Supplementary data protection agreement

to the license agreement for license ID: .....

between

.....  
.....  
.....

represented by .....

- Hereinafter referred to as the "**Client**" -

and

**Astaro Services AG**, Rheinweg 7, CH-8200 Schaffhausen

- Hereinafter referred to as the "**Contractor**" -

## Table of Contents

Preamble	3
§ 1 Subject and duration of this agreement	3
§ 2 Categories of affected individuals and types of saved data	4
§ 3 Rights and responsibilities of the Client	4
§ 4 General obligations of the Contractor	5
§ 5 Technical and organizational measures	8
§ 6 Amendment, blocking, and deletion of data	8
§ 7 Deletion of data and return of data carriers	8
§ 8 Damages	9
§ 9 Security interests	9
§ 10 General	9
Appendix I:	10
General technical and organizational measures	10

## **Preamble**

The Contractor was instructed to archive the Client's e-mails. This agreement concluded in this respect shall hereinafter be referred to as the 'principal agreement'.

Since the Contractor may be able to access the Client's personal data during the installation and adjustment of the storage system provided by the Contractor and during the subsequent maintenance and administration processes, commissioned data processing forms a part of this assignment. Since the Client is responsible for adhering to data protection regulations, the following must be agreed as a supplement to the principal agreement:

### **§ 1 Subject and duration of this agreement**

- 1) Insofar as it is relevant to this agreement, the principal agreement between the Contractor and Client relates to the archiving of e-mails. Astaro Mail Archiving ('AMA') offers to archive e-mails as a service provided by Astaro Services AG Rheinweg 7, CH-8200 Schaffhausen ('Astaro'). E-mails which are to be archived are transmitted in encrypted form to the archiving service which can be accessed centrally via the internet. The e-mails are then indexed, archived, and made available at any time for authorized user inquiries by the customer.
- 2) As a cloud-based solution, AMA offers excellent administration, scalability, availability, and security advantages. Astaro Group companies have many years' experience in internet security-related matters. This extensive expertise particularly enables Astaro to safeguard the data protection, access protection, and availability of AMA.
- 3) This document explains the internal processes and structure of AMA, as well as protective measures for comprehensive data and access protection.
- 4) The AMA infrastructure comprises a number of servers which process different types of task.
- 5) Astaro differentiates here between Production, Backup and Control Clouds whose operations are separated physically and geographically in separate hosting environments. This separation also serves to divide powers in order to maximize access and data protection.
- 6) This term of this commissioned data processing agreement is the same as that of the principal agreement, including any subsequent agreements, and shall expire on the same date as the principal agreement or the final subsequent agreement. This is without prejudice to the confidentiality obligations agreed in section 4 (2).

## § 2 Categories of affected individuals and types of saved data

The areas of activity/services specified in section 1 result may result in access to personal data. However, this is only in encrypted form.

## § 3 Rights and responsibilities of the Client

- 1) The Client alone is responsible for assessing the legitimacy of the data processed/collected/used and for safeguarding the rights of the individuals affected. The Client remains the owner of the data.
- 2) As far as access to personal data is concerned, the Client is authorized to issue the Contractor with instructions. The Client's data must be handled only according to the stipulations agreed (in both this agreement and the principal agreement) and the Client's instructions. The Client retains the right to issue instructions with regard to the methods, scope, and processes applied to the data processing and may substantiate this right in individual cases. Any changes to the data to be processed or to the procedures used must be agreed and recorded by both parties. The Contractor may only disclose information to third parties or affected individuals with the Client's prior written consent.

The following individuals will act as contacts for the execution of this agreement on behalf of each party:

On behalf of the Client:

.....  
[Name, contact details]

The data protection officer named in section 4 (1) shall act as the central point of contact for the Contractor.

Any changes must be immediately notified to the other contracting party.

If, in the opinion of the Contractor, an instruction infringes data protection regulations, the Contractor shall immediately inform the Client of this. In this case, the Contractor is entitled not to carry out the particular instruction until it has been confirmed or amended by the employees of the Client..

### 3) Inspection rights

The Client has the right, in agreement with the Contractor, to carry out the contractual inspections provided for by the law or assign these to other inspectors, to be named at a later date.

Before the data is processed and for the duration of this agreement, the Client is also entitled to ensure that the technical and organizational measures agreed upon are being adhered to by the Contractor. To this end, the Contractor shall provide evidence to the Client of the implementation of these technical and organizational measures, as described in the Appendix. Unless it relates only to this specific assignment, this evidence may be provided in the form of a recent certificate, reports or extracts from reports issued by independent authorities (such as financial auditors, data protection auditors, data protection officers, IT security officers, or quality auditors) or appropriate certification from an IT security or data protection audit (in accordance with the basic protection regulations set by the Federal Office for Information Security).

The Client has the right to carry out spot checks, for which prior notification should be given, unless this contravenes the purpose of the checks, to ensure that the Contractor's business operations comply with the terms of this agreement. On request, the Contractor shall provide the Client with the information it requires in order to effectively exercise its inspection rights and submit the relevant documents.

## § 4 General obligations of the Contractor

- 1) The Contractor has appointed a data protection officer who will carry out his duties in accordance with statutory regulations. This is currently:

Mr. André Meuser

Tel. +49 (89) 210977-10

HYPERLINK "mailto:andre.meuser@prw-consulting.de" [andre.meuser@prw-consulting.de](mailto:andre.meuser@prw-consulting.de)

The Contractor shall inform the Client in writing should there be a change to the person appointed as data security officer.

## 2) Data confidentiality

In the course of remote maintenance or on-site intervention, the Contractor undertakes only to access data to the extent required in order for it to carry out the services required and to the extent permitted by the following conditions.

The technical and organizational measures taken by the Contractor to process and store the Client's data must be designed to protect the confidentiality of the data at all times.

Should any stored data content be disclosed to the Contractor, the Contractor shall ensure that it remains confidential.

In fulfilling the agreement for the Client, the Contractor shall adhere to this confidentiality and data secrecy requirement and shall treat as confidential all knowledge of business and trade secrets obtained within the scope of this contractual relationship. The Contractor is required to ensure that all its employees who might come into contact with the Client's data agree in writing to maintain data confidentiality and provide evidence of this to the Client. The Contractor shall ensure that all individuals it assigns to process data or fulfill this agreement comply with the legal provisions applicable to confidentiality requirements and data protection and that any information obtained is not disclosed to third parties or exploited in any other way and to monitor the confidentiality obligations established in this way.

These obligations continue to apply after the end of the contractual relationship.

## 3) Subcontracting

The Contractor is permitted to subcontract work to the extent described in order to complete the assignment within the scope of this agreement. Further subcontracting is only permitted with Client's prior written consent. The Subcontractor should be subject to the same data protection requirements imposed on the Contractor by the Client.

The Contractor must also ensure that the Client can also exercise its inspection rights over the Subcontractor.

4) Obligation to inform

The Contractor acknowledges that there is a statutory obligation to report any loss, unlawful transfer, or disclosure of personal data, should this arise. Should the Contractor suspect or have specific evidence that the Client's personal data has been disclosed to unauthorized third parties, it shall inform the Client of this, regardless of the cause.

This obligation shall also apply in the event of serious disruption to operating procedures, any suspected infraction of personal data protection regulations, or other irregularities in the handling of the Client's personal data. The Contractor and the Client must mutually agree appropriate measures to safeguard the data and minimize the potentially negative consequences for the Client or the individuals affected.

5) Economical use of data

The Contractor shall restrict all access to the Client's data to the minimum level stipulated in the primary agreement. Should it be absolutely essential to access personal data, the Contractor must inform the Client before this data is accessed. The Client shall decide how to proceed in such an event.

Should the Client grant access to certain personal databases, the agreed work may only be carried out on these databases.

If personal data is accessed during the performance of the agreed maintenance work, it may not be changed. Any changes made in error must be reported to the client.

Changes to system files required in the course of the work must be recorded by the Contractor. At the request of the Client, these changes must be reversed once the work has been completed.

6) Transfer of memory content

Should the assignment comprise the copying of saved data, the Contractor should employ a method that prevents the content of the databases from being displayed as far as possible.

If original data is extracted for error analysis during the maintenance work, this data must be deleted once the procedure is complete.

## **§ 5 Technical and organizational measures**

The Contractor is obliged to implement technical and organizational measures and adhere to them for the duration of this agreement. The Contractor shall document these measures.

Should an inspection by the Client reveal the need to adjust these measures, this adjustment shall be carried out immediately by the Parties.

These individual measures are set out in **Appendix 1** to this agreement.

## **§ 6 Amendment, blocking, and deletion of data**

The Contractor may only amend, delete, or block data that is processed during the assignment if instructed to do so by the Client. Should affected individuals contact the Contractor directly and request the amendment or deletion of their data, the Contractor shall immediately report these requests to the Client and, if necessary, support the Client in taking any measures required.

## **§ 7 Deletion of data and return of data carriers**

At any time requested by the Client, but at the latest upon the expiry of the agreement, in accordance with data protection regulations, the Contractor shall return to the client or destroy with prior approval all documents, processing and usage results, and databases acquired in the course of the contractual relationship. The same applies to test and waste material. The deletion report must be submitted to the Client without being requested.

Documentation demonstrating that data has been processed correctly and in accordance with the agreement must be retained by the Contractor for the appropriate period after the end of the agreement. For the Contractor's convenience, it may be handed over to the Client when the agreement ends.

**§ 8 Damages**

Should the content of databases be disclosed to third parties, in breach of the confidentiality requirements, the Contractor must compensate the Client for any damages that may arise in accordance with the principal agreement.

The Contractor shall be liable for the errors of its personnel in the same way that it is liable for its own errors.

**§ 9 Security interests**

Should the Client's property be put at risk by the Contractor through the actions of third parties (such as seizure or confiscation), bankruptcy or insolvency proceedings, or through other events, the Contractor must immediately inform the Client.

**§ 10 General**

- 1) Should individual provisions of this agreement be invalid, this shall be without prejudice to the effectiveness of the remaining provisions of the agreement.
- 2) No ancillary verbal agreements may be made to this agreement. Any amendments or addenda must be made in written form in order to be valid. This shall also apply to the removal of this written form requirement.
- 3) This Contract is subject to German Law. UN private law and legislation on contracts for the sale of goods. The place of jurisdiction is Karlsruhe. However, Astaro reserves the right to take legal action against the Client at the court with jurisdiction over its registered office, as well.

....., on (date) .....

.....  
(Client)

.....  
(Contractor)

## Appendix I:

### General technical and organizational measures

Private bodies which collect, process, or use personal data themselves or on behalf of a third party must implement the necessary technical and organizational measures to ensure compliance with EU data protection regulations. Measures are only required if the effort involved is in proportion to the protection required.

The law defines various types of control that enable legal requirements to be met. These shall be implemented as follows by the Contractor:

#### 1) Access control

Access to data processing equipment with which personal data is (or may be) processed or used should be denied to unauthorized persons. The Contractor must therefore ensure that unauthorized persons cannot access areas in which the Client's data is processed or saved and cannot view or access data processing equipment (monitors, printers, and so on) used to process or display the Client's data.

Measures taken by the Contractor in order to comply with this obligation:

The operator's building is accessed through a door in the entrance hall which can only be opened using a transponder and a PIN. Images of everyone who accesses this room will be captured on video camera. The images from this camera will be recorded and saved for a limited period. Likewise, individual server rooms can only be accessed by specially authorized individuals using a transponder and PIN code.

If data is processed at external data processing facilities, access control (such as backup) is provided by means of ID checks and secure access zones protected using code cards and PINs.

#### 2) Access control

Unauthorized individuals must not be permitted to access the Contractor's data processing systems. The Contractor must therefore provide individuals employed to carry out the services specified in the principal agreement with a secure user ID.

Measures taken by the Contractor in order to comply with this obligation:

Access to the computing center resources is restricted through a strict domain access policy. Identification and authentication at the domains is provided through a username and a complex individual password which must be changed regularly. Failed

unauthorized access attempts will be recorded and monitored. If the user is absent, the system is automatically locked.

3) Access control

It should be ensured that only individuals working to fulfill the principal contract are able to access the Client's data. In addition, appropriate access rights should be established (profiles, groups, roles, and so on). These rights should be granted purely on a need-to-know basis.

Measures taken by the Contactor in order to comply with this obligation:

Rights are only granted after approval and purely on a need-to-know basis. As far as technology allows, personal accounts will be used for administration. Every user account is therefore assigned to just one person.

Rights are allocated according to roles or, as recommended by Microsoft, nested within resource and authorization groups. This makes both changes to rights and regular monitoring easier.

4) Transfer control

The Contractor must ensure that the Client's personal data is not read, copied, altered, or removed by unauthorized individuals during its electronic transfer, transport, or storage on data carriers.

Personal data may only be transferred and saved via e-mail in encrypted form.

Personal data may only be saved, sent, or transported (such as when the data is issued by the Client) on mobile data carriers (DCs, USB sticks, disks, memory cards, and so on) in encrypted form.

During remote maintenance or service procedures, the Client's data may only be accessed via secure, encrypted connections.

The secure transfer modes and encryption methods should be regularly updated according to the recommendations in the data protection manual issued by the BSI (Federal Office for Information Security).

Measures taken by the Contactor in order to comply with this obligation:

Data transferred by the client is transported and saved in encrypted form. The relevant areas of the data carriers are encrypted using data and hard drive encryption

software. Only encryption procedures considered secure by the BSI are used to do this (such as AES256).

5) Input control

The Client must ensure that it is possible to verify and establish at a later date whether and by whom personal data was input, edited, or removed from the data processing system. Appropriate reporting systems must therefore be in place for these activities.

Measures taken by the Contactor in order to comply with this obligation:

The Contractor uses reporting systems that record and safeguard data access, storage, and data protection.

6) Order control

The Contractor must ensure that the Client's personal data is only processed according to the Client's instructions. If the Contractor employs a subcontractor, the subcontractor must be obliged to follow the instructions and comply with the data protection requirements in the same way as the Contractor.

Measures taken by the Contactor in order to comply with this obligation:

Appropriate processing and change processes have been established to ensure that customer orders are handled correctly. Changes are only carried out in a controlled procedure and with notification from the Contractor.

## 7) Availability control

The Contractor must ensure that the Client's personal data cannot be lost or destroyed. This requires the following safety measures, in particular:

- Implementation of appropriate data protection methods such as tape backup, data mirroring, snapshots, and so on.
- Physical separation of the backup data.
- The use of uninterrupted power supplies to ensure that data is not lost during storage or transfer.
- Implementation of security measures that prevent access by unauthorized third parties (virus protection, firewall, spyware detection, packet filters, and DMZs, for example).
- The creation of emergency plans.

Specific measures taken by the Contractor in order to comply with this obligation:

In order to provide the highest possible levels of availability, the Contractor uses a variety of technologies and processes.

So that data can be restored in an emergency, data is regularly backed up in archive networks in different geographical locations to the storage centers. Data stored in the archive is always saved using redundant systems.

To ensure an uninterrupted supply of power to the system, redundant power supply units are built into the systems wherever possible. The power supplied to the systems is backed up using uninterrupted power supplies.

Security measures are in place to prevent intrusion from unauthorized third parties. All links to unsafe networks (such as the internet) are protected using firewall systems.

The relevant security measures are regularly updated in line with developments in technology.

## 8) Separation

The Client must ensure that data extracted for different purposes is also processed separately.

The data must be separated in such a way that it cannot be confused with data belonging to other contractual partners or clients of the Contractor or be accessed by unauthorized third parties (even unintentionally).

Should data belonging to other contractual partners or clients of the Contractor be accessed or confiscated by the authorities, it must be ensured that the Client's data is not affected.

The Client's data may not be used for test purposes.

Measures taken by the Contractor in order to comply with this obligation:

To separate network traffic created by different clients, all data is encrypted using an encryption certificate that is unique to each client. It is therefore not possible to access data belonging to one client directly from data belonging to another client. Furthermore, the encryption certificates are only kept in the main memory of the processing system during the processing period and cannot be viewed by third parties.