ALLNET Computersysteme GmbH

ASP/SaaS Data Processing Agreement

Date 09.07.2021 Version 1.1

This data processing agreement applies to the use of all products of Allnet Computersysteme GmbH, Maistraße 2, 82110 Germering (hereinafter: "**ALLNET**" as processor) we provide our customers (hereinafter: "**customer**" as controller and principal) by way of the Application Service Providing ("ASP") or as Software as a Service ("SaaS") and for which we process personal data.

Preamble

This agreement supplements and substantiates the obligations of the parties under contracts concluded with us for the use of ASP/SaaS services where employees of the processor or agents of the processor may come into contact with personal data within the meaning of Article 4 (1) GDPR of the customer with respect to data protection.

1. Subject matter, duration and specification of data processing

1.1. The subject matter, type and purpose of data processing is defined in the individual contracts and the respective specifications of services.
1.2. Depending on the type of contract, processing involves the following types of data: personal master data, communication data, timestamps, media contents, measurement data, configuration data and other personal data.
1.3. Processing applies to the following categories of persons: for contracts with consumers: the contracting party as the holder of the user account; for contracts with businesses: managing directors, executive staff, employees; for enterprise and white label licenses: furthermore customers or subscribers of the customer, other data subjects.
1.4. The term of this agreement is based on the booking period of the individual contracts, unless further obligations are stipulated in this agreement.

The contracted data processing takes place in the European Economic Area. The customer agrees to ALLNET relocating to a third country provided the special requirements under Article 44 et seqq. GDPR are met.

2. Scope and confidentiality

2.1. ALLNET processes personal data on behalf of the customer. This includes activities substantiated in the individual contracts and the specifications of services. With respect to data processing, the customer remains liable for compliance with the legal provisions on data protection, in particular the lawfulness of data processing.

2.2. ALLNET solely processes data as instructed by the customer. The instructions consist of the instructions originally defined in the individual contracts and the specification of services. The customer may change instructions within the respective functionality directly through administration of a user account, or otherwise in written form or in text form to ALLNET.

2.3. ALLNET will promptly notify the customer if ALLNET believes an instruction violates data protection regulations. ALLNET is entitled to suspend the implementation of the respective instruction until the instruction has been confirmed or changed by the customer.

3. Processor obligations

3.1. ALLNET may only process personal data of data subjects as instructed by the customer. In the event ALLNET is obligated to process data otherwise under national or European law, ALLNET will notify the customer of this fact prior to such processing, provided the respective law does not prohibit such notification for important reasons of public interest.

3.2. ALLNET will design the internal organisation within its sphere of responsibility in compliance with data protection, in particular through the technical and organisational measures ("TOMs") specified in Annex 1 to ensure adequate protection of the personal data.

The measures to ensure confidentiality, integrity, availability and resilience of systems and services associated with processing personal data. The customer is aware of these technical and organisational measures. It assumes responsibility for these offering an adequate level of protection for the risks of the personal data to be processed.

3.3. ALLNET reserves the right to change technical and organisational measures using equitable discretion, however guarantees they will at a minimum meet the level of protection required by law and under the contract.

3.4. Within the scope of the performance owed under the contract, ALLNET will assist the customer with the fulfilment of requests and demands of data subjects pursuant to Chapter III of the GDPR as well as compliance with the obligations specified in Article 33 to 36 GDPR. ALLNET may demand an appropriate fee for this.

3.5. ALLNET avouches employees processing personal data of the customer and other persons working for ALLNET are prohibited from processing personal data outside the instructions of the customer. ALLNET further guarantees the persons authorised to process personal data are bound to confidentiality or under an appropriate statutory obligation of secrecy. The duty of confidentiality or secrecy continues after completion of the assignment.

3.6. ALLNET will promptly notify the customer if it becomes aware the customer's personal data has been breached. ALLNET shall take the necessary measures to protect the personal data and to minimise the potential negative outcome for the data subjects.

3.7. ALLNET us obligated to appoint a competent and reliable data protection officer pursuant to Article 37 GDPR insofar and as long as the statutory requirements for the obligation of appointing said person are given. The customer will be provided the contact information for said for the purpose direct contact. Contact information for the primary point of contact in data protection matters and the data protection officer are published in the privacy policy.

3.8. ALLNET guarantees to fulfil the obligations under Article 32 (1) (d) GDPR and to implement a process to regularly review the effectiveness of technical and organisational measures to ensure the security of processing.

3.9. The customer is responsible for correcting and erasing personal data. The same applies to restricting the processing of personal data.

3.10. The personal data will be erased at the end of the booked period. The customer is responsible for backing up its personal data and to move the personal data prior to the end of the contract. Unless otherwise stipulated in the individual contracts, ALLNET is under no obligation to release personal data the customer can access itself.

3.11. ALLNET undertakes to keep a record of processing activities pursuant to Article 30 (2) GDPR.

4. Customer obligations

4.1. The customer is responsible for providing ALLNET with the personal data in due time for performance of services. The customer is solely responsible for the quality of personal data. The customer shall notify ALLNET promptly and fully if it determines errors or irregularities related to data protection provisions when reviewing the processing result.

4.2. In the event a data subject makes any claims under Article 82 GDPR, the customer and ALLNET undertake to assist each other in defence against such claims. Contact information for the primary point of contact in data protection matters and the data protection officer are published in the privacy policy.

5. Requests of data subjects

In the event a data subject contacts ALLNET with requests related to the correction, erasure, restriction of processing or information related to personal data, ALLNET will promptly forward this request to the customer if able to allocate to the customer based on the information provided by the data subject.

6. Proof

6.1. ALLNET shall on request provide the customer with proof of compliance with the obligations under Article 28 GDPR and this contract through appropriate means.

6.2. In the event further reviews by the customer or an auditor commissioned by said are required, any requests must be submitted in writing. ALLNET is entitled to require an appropriate non-disclosure agreement first be signed by the customer or the auditor commissioned by said. In the event auditors commissioned by the customer are in competition with ALLNET, ALLNET shall be entitled to object. The objection shall be submitted to the customer in text form.

6.3. In the event of an audit by a supervisory authority for data protection or other sovereign supervisory authority of the customer, 6.2 on principle applies accordingly. Signing a non-disclosure agreement is not required if this supervisory authority is bound to professional or legal confidentiality.

6.4. ALLNET is entitled to demand appropriate fee for assisting with an audit pursuant to 6.2 or 6.3 unless the reason for the audit is strong suspicion of a data breach within the sphere of responsibility of ALLNET. In this case, the customer shall demonstrate probable cause for the suspicions when announcing the audit.

7. Contractors (other processors)

7.1. The customer agrees to ALLNET using contractors. If contractors are already used initially, ALLNET shall provide the customer the corresponding list with their full address prior to data processing taking place. Before engaging additional or replacing existing contractors, ALLNET shall notify the customer in text form at least 4 weeks in advance. The customer may only object to the engagement or replacement within 14 days for good reason. If the customer does not object within this period, the engagement or change is considered approved. If good reason exists which ALLNET cannot correct by amending the assignment, the customer is entitled to extraordinary cancellation of this contract and the related individual contract. If ALLNET submits assignments to contractors, ALLNET shall also transfer the data protection obligations under this contract to the contractor.

7.2. On written request of the customer, ALLNET shall provide information related to the data protection obligations of its contractors.

7.3. The provisions of this point 7 also apply when engaging a contractor in a third country in compliance with the requirements of Article 44 et seqq. GDPR.

8. Liability

8.1. The liability provisions of the individual contracts apply.

8.2. The customer indemnifies ALLNET of all third-party claims against ALLNET for infringement of their rights due to the processing of personal data commissioned by the customer unless the third-party claim is based on ALLNET processing personal data contrary to instructions.

9. Information obligations, written form, choice of law

9.1. In the event the personal data of the customer in the possession of ALLNET is at risk through attachment or confiscation, insolvency or settlement procedures, or due to other events or measures of third parties, ALLNET shall immediately notify the customer. In this context, ALLNET shall immediately inform the third party the sovereignty and ownership of the personal data solely lies with the customer as the controller within the meaning of the GDPR.

9.2. Amendments and addenda to this agreement must be made in writing, which can also be in text form. This also applies to waiving this requirement for form.

9.3. In the event of conflicts, the provisions of this data protection agreement take precedence over those of the individual contract.

ALLNET Computersysteme GmbH

ANNEX TO THE DATA PROCESSING AGREEMENT (AVV) - TECHNICAL ORGANISATIONAL MEASURES "TOMs"

Date 09.07.2021 Version 1.1

The following technical and organisational measures have been implemented by ALLNET as the processor and agreed with the customer.

1. Measures to pseudonymise and encrypt personal data

1.1. Pseudonymisation

“Pseudonymization" means the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the provision of additional information, provided that such additional information is stored separately and is subject to technical and organizational measures ensuring that the personal data is not attributed to an identified or identifiable natural person.

Our measures within the context of pseudonymising personal data consist of:

☐ Selecting a suitable state-of-the-art pseudonymisation procedure

☐ Pseudonymisation requirement is a central component within the context of the company's data protect concept

☐ Pseudonymisation of data following a risk-based approach pursuant to different security requirements of data

☐ Using software which enables secure management of pseudonymised data

☐ Secure storage of cryptographic keys or checklists (if applicable encrypted storage of checklists) used for pseudonymisation

☐ Authorisation concept for access to cryptographic keys or checklists which allow personalisation

1.2. Encryption

Encryption means a process which converts plain text information into an unreadable or uninterpretable character string.

Our measures related to encrypting data consist of:

☐ Encrypting confidential data during transfer and over data networks

☐ Encrypting confidential data during storage on IV devices and mobile data storage media

☐ Encrypting strictly confidential data stored on data storage media (hard disks)

☐ Performing a risk analysis if cryptographic measures are not feasible

☐ Instructions on the use of coordinated and approved cryptographic procedures

☐ Algorithms, applications and standards

☐ Key material for production systems issued by a Public Key certification authority

☐ Non-disclosure of private keys for a certificate

☐ Protecting from unauthorised access or spying out secret keys and the private keys of the Public Key cryptography

☐ Secure erasure or destruction of keys which are no longer required

2. Measures to ensure confidentiality

Measures to implement the confidentiality requirement include those related to entry, data usage or access control. The technical and organisational measures taken in this respect are intended to ensure an appropriate level of security for personal data, including protecting from unauthorised or unlawful processing, accidental loss, accidental destruction or corruption.

2.1. Entry control

2.1.1. Entry of ALLNET business premises

☐ Measures implemented to prevent unauthorised entry of ALLNET business premises where personal data is processed or used.

☐ Further security measures (e.g. video surveillance, monitoring the door status of entries, exits and emergency doors, securing the perimeter with fencing, plant security) may be implemented depending on the risk classification of the respective site

☐ Identifying authorised persons

☐ Entry control equipment using personalised and coded IDs, personally issued keys

☐ Entry rules for external persons

☐ Establishing different security zones with different access authorisation

☐ Documenting the issuance and revocation of access rights

☐ Video surveillance

☐ Burglar alarm with alarm transmission to the permanently staffed security control centre or to the police

☐ Monitoring the door status of entries/exits

☐ Monitoring the emergency door

☐ Restrictive key rules

☐ Visitors only permitted accompanied by ALLNET employees

☐ IDs must be worn

2.1.2. Access to ALLNET server rooms

Measures taken in addition to the above security measures to prevent unauthorised access to ALLNET server rooms where personal data is processed or used are listed below. Additional security measures (e.g. video surveillance) may be implemented depending on the risk classification of the respective ALLNET server room.

☐ Logging entry of server rooms (automatically through entry control system or lists set out)

☐ Video surveillance inside the server room

☐ Monitoring the door status for server rooms

☐ Automatic door closure on server room entries and exist

☐ Outside companies/technicians only permitted inside server rooms in the constant company of ALLNET employees

2.1.3. Data access control

Measures to prevent unauthorised use of data processing system

Requirements for setting passwords:

☐ Minimum length

☐ Use of characters (symbols, special characters, numbers)

☐ Use of trivial passwords

☐ Change intervals

☐ Sharing passwords prohibited

☐ Storage and transmission to data processing systems

Requirements for the applications for managing passwords to be used

☐ Screen lock if inactive for defined amount of time

☐ Locking out user names or delaying sign in attempts after multiple failed sign in attempts

☐ Regular review of access authorisation for user access to the network for:

☐ Employees

☐ External parties

Regular review of access authorisation for administrators of:

☐ Networks and network services

☐ Servers

☐ Risky applications

☐ Partitioning internal networks by setting up firewall systems

☐ Using Virtual Private Networks (VPN) with user/password as authentication feature

☐ Machine certificate as authentication feature

☐ Restrictive requirements for disabling USB ports

☐ Using a central administration software for smartphones (e.g. to delete data from

the smartphone)

2.1.4. Data usage control

Provisions which ensure that only persons authorised to use a data processing system can access information within their access authorisation and that personal data cannot be read, copied, altered or deleted during processing, use or after being saved.

☐ Using user-specific, unique credentials

☐ Authorisation concept on an application layer with different authorisation levels (e.g. roles)

☐ Logging access permissions assigned

☐ Use of signatures and certificates to ensure authorship

☐ Data protection compliant destruction of data, data storage media and printouts based in correspondence with protection class concept

2.2. Separation control

Measures which ensure data collected for different purposes can be processed separately.

☐ Logical or technical data separation

☐ User profiles / separation of user accounts

☐ Different access permissions

☐ Storage on specific drives

☐ Separating processing systems

3. Measures to ensure integrity

Measures to implement the integrity requirement are on one hand those which also fall under input control, and on the other hand those which generally contribute to prevent unauthorised or unlawful processing, destruction or accidental damage.

3.1. Transmission control

Measures to ensure that personal data cannot be read, copied, modified or removed by unauthorised parties during their electronic transmission, transport or storage on data carriers and that it is possible to check and determine to which parties a transmission of personal data by data transfer equipment is provided for.

☐ Encrypting data and data storage media based on their need for protection, particularly in form of hardware- and software-based file and hard disk encryption.

☐ Encrypting data transmission based on their need for protection, particularly during transmission over public networks.

☐ Using Virtual Private Networks (VPN)

☐ During physical transport: Using secure, lockable transport containers during

☐ Transport of backup data storage media

☐ Data protection compliant destruction of data, data storage media and printouts based in correspondence with

☐ the protection class concept

☐ Careful selection of transport personnel

3.2. Input control

Means measures to ensure the ability to later review and determine if and by whom personal data was entered, changed or removed from data processing systems.

☐ Contract design in compliance with the law with respect to contracts with contractors on the processing of personal data with the corresponding provision on control mechanisms

☐ Obtaining self-disclosures from service providers on their measures to implement requirements under data protection law

☐ Written confirmation of verbal instructions

☐ Recording and adequate provision of suitable actions (e.g. log files)

☐ Use of logging and log analysis systems

☐ Defining those authorised to create data storage media and processing data

4. Measures to ensure availability and resilience

4.1. Availability control

Means measures to ensure personal data is protected against accidental destruction or loss. These measures must be designed to ensure long-term availability.

☐ Central hardware and software procurement

☐ Using centrally reviewed and approved standard software from secure sources

☐ Regular data backups or mirroring

☐ Hardware (particularly servers) are taken out of service after reviewing their data storage media and if necessary backing up the relevant datasets

☐ Uninterruptible power supply (UPS) in the server room

☐ Separate storage of data collected for different purposes.

☐ Multilayer antivirus and firewall architecture

☐ Disaster recovery (disaster recovery for security and data breaches with specific instructions)

☐ Fire/water and temperature early warning system in server rooms

☐ Fire doors

☐ IT supported by qualified and continuously trained employees

☐ Regular data recovery tests in compliance with the security concept

4.2. Order supervision

Means measures to ensure personal data processed by a contractor of ALLNET can only be processed in compliance with the instructions and standards for processing customer data.

Define criteria for selecting the contractors (references, certifications, quality seals)

☐ Detailed written definition (contract/agreement) of contractual relationships and formalisation of the entire order process, including the use of contractors, clear provisions on responsibilities

☐ Ensuring the fulfilment of the contract is monitored and documented

☐ Contractual agreement with contractors obliging internal and external staff to confidentiality

4.3. Resilience test

This includes measures the provider must already take during the stage prior to data processing. In addition, systems must also be continuously monitored.

☐ Load balancing

☐ Dynamic processes and memory upgrade

☐ Penetration tests

☐ Regular stress test on data processing systems

☐ Maximum capacity of the respective data processing system beyond the required minimum in advance

☐ Regular employee training to act in compliance with the requirement to ensure integrity and confidentiality of data processing

5. Measures to restore availability

Ensuring restorability on one hand requires adequate safeguards as well as action plans which can restore operation in the sense of catastrophe scenarios.

☐ Regular data backups and mirroring

☐ Redundant data storage

☐ Dual IT infrastructure for processing with high availability standards

☐ Backup data centre in the case of sabotage or critical environmental incidents

6. Procedure for regular review, assessment and evaluation

A regular review, assessment and evaluation of the effectiveness of technical and organisational measures to ensure secure processing are carried out through:

☐ Internal reviews by the competent departments (e.g. audit, data protection office, information security officer, process controls by Quality Management)

☐ External reviews by auditors, certification authorities