Data Processing Agreement

Annex to the Agreement

by and between

Licensor

- hereinafter referred to as "**Processor**" -

and

Licensee

- hereinafter referred to as "**Controller**" -

Content

1 Definitions

Definitions made in the Agreement (hereinafter referred to as "Main Contract") shall also apply to this Data Processing Agreement (hereinafter referred to as "DPA"), unless otherwise expressly provided herein. If the term "data" is used in this DPA, this always refers to personal data within the meaning of Art. 4 no. 1 GDPR. Otherwise, the terms used in this DPA shall be understood as defined in the GDPR or in other laws (e.g. § 2 BDSG (German Federal Data Protection Act), § 2 TMG (German Telemedia Act)).

2 Subject Matter and Term of Processing

2.1 In accordance with the Main Contract, Processor shall provide Cognigy.AI SaaS Services to Controller in relation to Conversational AI Software and in this context shall also be the recipient of personal data (hereinafter referred to as "Order"). It cannot be ruled out that Processor may gain access to personal data and process such data on behalf of Controller when providing the Cognigy.AI SaaS Services. Processor processes the personal data in connection with the Order exclusively within the framework of the provisions of this DPA. Processor shall not process the personal data concerned for any other purpose and in particular not for own purposes.

2.2 Solely Controller determines the purposes and means of the processing. Changes to the subject of processing and changes to processing itself shall be agreed upon jointly and shall be specified in writing by amending this DPA.

2.3 The term of this DPA corresponds to the term of the Main Contract.

3 Order Details

Regarding the order processing, the content of the Order is detailed as follows:

Nature and purposes of processing	Processor will process personal data as necessary to perform the Cognigy.AI SaaS Services pursuant to the Main Contract, as further specified in the documentation, and as further instructed by Controller in its use of the Cognigy.AI SaaS Services.
Type of personal data	*All personal data that the Controller provides in the context of his individually selected use of the* Cognigy.AI SaaS services*. These are e.g. personal master data, communication data (e.g. telephone, e-mail) contract master data (contractual relationship, product or contract interest), customer history, contract billing and payment data, planning and control data, special categories of personal data*
Categories of data subjects	*Depends on the personal data that the Controller provides in the context of his individually selected use of the* Cognigy.AI SaaS Services. These may be *Customers, prospects, subscribers, employees within the meaning of section 26 BDSG (German Federal Data Protection Act), suppliers, commercial agents, contact persons*

4 Authority to Issue Instructions

4.1 Processor shall only process the personal data on the documented instructions of Controller. This shall also apply to the transfer of personal data to a third country or an international organisation, unless Processor is obliged to do so by the law of the European Union or of the Member States to which it is subject; in such a case, Processor shall inform Controller of that legal requirement in text form (e.g. by e-mail or fax) before processing, unless that law prohibits such notification on important grounds of public interest.

4.2 Controller has the right to issue instructions to Processor within the scope of the subject matter of the Order (see section 2) regarding the type, scope and procedure of the processing of personal data. It may specify its instructions by means of individual instructions. Instructions given orally must be confirmed

by Processor immediately in writing or in text form. In this context, instructions shall be understood to mean an order issued by Controller that instructs Processor how to handle the processing of personal data in a special case (e.g. anonymization, correction, restriction of processing, deletion, surrender).

4.3 Controller shall document all instructions given to Processor. Controller shall make the documentation available to Processor for each instruction issued. However, Processor shall be responsible for documenting the implementation of the instructions issued by Controller.

4.4 Processor shall at all times comply with the relevant instructions of Controller. As long as and to the extent that Processor processes personal data resulting from the Order beyond its expiration, Processor shall continue to follow Controller's instructions even after expiration of this DPA; Controller shall bear all expenses and costs incurred by Processor as a result of following such instructions.

4.5 Processor shall take all necessary steps to ensure that the natural persons under its authority who have access to personal data do not process them except on the instructions of Controller, unless they are required to do so under Union or Member State law.

4.6 In the event of a change of contact or a longer-term prevention of the contact person, the successor or the representative must be notified to the other party in writing without undue delay. If instructions modify, cancel or supplement the stipulations made in section 3, they are only permissible if a corresponding modification to this DPA in text or written form has been made beforehand.

4.7 Processor shall immediately inform Controller if, in Processor's opinion, an instruction issued by Controller violates statutory provisions and in particular the GDPR, the BDSG or other applicable data protection provisions of the European Union or its Member States. Processor is entitled to suspend the execution of the corresponding instruction until it has been confirmed or amended by a person of Controller who is authorized to issue instructions.

5 Confidentiality Duties

5.1 Processor shall only employ employees for the processing of personal data if Processor has familiarized them with the provisions of data protection law applicable to them and has bound them in writing - also beyond the termination of their employment - to confidentiality; the text form is not sufficient. A commitment to confidentiality is not required if employees are subject to an appropriate statutory duty of confidentiality.

5.2 Processor shall monitor compliance with data protection regulations by its subordinated persons who have access to personal data. Processor shall regularly train its employees, who are entrusted with the processing of personal data, to an appropriate extent and at appropriate intervals and shall sensitize them for data protection.

5.3 Controller shall treat all knowledge of trade and business secrets as well as data and other IT security measures of Processor that Controller has received in the context of the order, in particular the technical and organisational measures of Processor, in strict confidence and shall not pass them on or use or disclose them in any other way. This applies to any unauthorized third parties, i.e. also to Controller's own unauthorized employees, if the disclosure or other utilization or disclosure of such information is not necessary for the proper fulfilment of the contractual or legal obligations of Controller. In any case of doubt, Controller shall obtain the written consent of Processor before such a passing on or other utilisation or disclosure.

5.4 Notwithstanding the confidentiality obligations agreed in section 5.3 of this DPA, Controller may disclose technical and organisational measures of Processor concerning the order within the scope of the legally imposed accountability to entitled persons and bodies (e.g. supervisory authorities), insofar as it is legally obliged to do so.

6 Technical and Organisational Measures

6.1 Processor shall implement appropriate technical and organisational measures for the Order, taking into account the nature, scope, context and purposes of the processing, as well as the risk of the varying likelihood and severity for the rights and freedoms of the data subjects, to ensure and prove that the processing is carried out in accordance with this DPA.

6.2 The data protection precautions of Processor attached as Appendix 1 (Technical and Organisational Measures), which contain the stipulations in accordance with Art. 32 GDPR, shall be set as a binding

minimum for executing the Order, which may not be fallen short of at any time. Processor undertakes to comply with the technical and organisational measures laid down in Appendix 1.

6.3 If, during the term of the Order, Controller determines that the risks to the rights and freedoms of the data subjects have changed, Controller shall inform Processor without undue delay so that Processor can adapt its technical and organisational measures in such a way that the level of data protection required for executing the Order remains safeguarded; the one-off and recurring expenses and costs incurred by Processor as a result of the adaptation shall be borne by Controller. As soon as Processor has specified the updated technical and organisational measures in Appendix 1, this new Appendix 1 shall replace the previously valid Appendix 1. Should a corresponding adjustment of the technical and organisational measures not be possible, unreasonable or even inadmissible for Processor, this shall constitute a good cause for both parties, entitling them to extraordinary termination for cause of the Main Contract including this DPA.

6.4 Processor shall ensure that the personal data processed under the Order are strictly separated from other data stocks. Detailed requirements and measures for separation are laid down in the technical and organisational measures in Appendix 1.

6.5 If and to the extent that Processor is obliged to provide evidence of the technical and organisational measures taken, it may submit evidence of compliance with approved codes of conduct pursuant to Art. 40 GDPR or of current certification pursuant to Art. 42 GDPR in order to support its evidence. Furthermore, Processor may also provide this proof by means of current certificates, reports or extracts from reports from independent bodies (e.g. auditors, revision, data protection officer, IT security department, data protection auditors, quality auditors) or a suitable certification by means of an information security or data protection audit (e.g. according to baseline security of the BSI (Federal Office of Information Security) or as part of an ISO 27001 certification).

6.6 The technical and organisational measures must be adapted to technical and organisational further development in the course of the contractual relationship. For this purpose, the technical and organisational measures agreed in Appendix 1 shall be reviewed at least once a calendar year by Controller and Processor in the light of section 6.1 and taking into account the state of the art. Changes resulting from such inspections shall be specified in writing. If, during the term of the Order, Processor determines on its own initiative that the measures taken by Processor do not or no longer adequately cover the risks to the rights and freedoms of the data subjects, Processor shall notify Controller. The provisions agreed in section 6.3 shall apply *mutatis mutandis* to the adaptation of Appendix 1.

7 Engagement of Sub-Processors

7.1 Controller herewith authorizes Processor in general to engage sub-processors.

7.2 Processor shall inform Controller before Processor engages sub-processors (chain order processing) or replaces sub-processors. Processor shall inform Controller of any intended changes concerning the addition or replacement of sub-processors, thereby giving Controller the opportunity to object to such changes. If Controller wishes to object to such changes, it shall notify Processor in writing within two (2) weeks after receipt of the information or without undue delay after becoming aware of a reason for objection when such a reason arises later. The provisions of this section 7 shall apply *mutatis mutandis* to any involvement or replacement of further sub-processors within the framework of a multi-stage chain order processing.

7.3 Processor shall impose on sub-processors, by contract or other legal instrument under Union law or the law of the Member State concerned, the same data protection obligations as those laid down in this DPA between Controller and Processor. In this context Processor shall ensure that appropriate technical and organisational measures are also implemented by the sub-processor in such a way that the processing complies with the legal requirements of data protection law.

7.4 On the effective date of this DPA, Controller has given its consent that Processor may deploy the subprocessors listed in Appendix 2 (Sub-processors) including their names and specific engagement for the processing of personal data to the extent specified therein.

7.5 Where Processor uses third party services as an ancillary service only to support the execution of the Order, this shall not be deemed to be the deployment of sub-processors within the meaning of this section 7. This includes, for example, cleaning staff, telecommunications services and postal services.

8 Assistance of Controller

8.1 Processor supports Controller in its duty to process and respond to requests of data subjects who exercise their rights set out in article 12 to 22 GDPR and sections 32 to 37 BDSG. For this purpose, the Processor shall, upon request, provide Controller with all relevant information available to Processor in the individual case. If a data subject applies directly to Processor to exercise the rights set out in Art. 12 to 22 GDPR and sections 32 to 37 BDSG, Processor will refer the data subject to Controller.

8.2 Processor may only disclose information to third parties or the data subject concerned with the prior written consent of Controller.

8.3 Processor shall take appropriate technical and organisational measures to be able to assist Controller as set forth in section 8.1 above.

8.4 Processor assists, with the information at its disposal, Controller in ensuring compliance with the obligations pursuant to Art. 32 to 36 GDPR.

8.5 Controller shall reimburse Processor for all expenses and costs incurred by Processor in assisting Controller.

9 Return and Deletion of Data

9.1 After the end of the provision of services relating to the Order, Processor shall return to Controller all personal data containing documents and processing results, that have been come in Processor's possession in connection with the Order as well as all personal data processed within the scope of the provision of the Cognigy.AI SaaS services. The aforesaid obligation to return means that Controller has at its disposal all personal data from and in connection with the Order after the return has taken place. The relevant storage media of Processor shall be deleted in conformance with data protection regulations after the return of the personal data. Controller can waive the return in whole or in part and instead demand the destruction or deletion of the documents, work results and personal data even without prior return. Test and scrap material shall be destroyed or returned to Controller. Physical destruction shall be carried out in accordance with DIN 66399, with at least protection level 2. Processor must confirm the destruction or deletion to Controller, stating the date.

9.2 Documentations which serve as proof of the orderly and proper data processing shall be stored by Processor in accordance with the respective retention periods beyond the termination of the contract. The same shall apply where there is an obligation to store personal data under Union law or the law of the Member States which Processor has to comply with.

9.3 If, after the end of the provision of services relating to processing, Processor incurs additional expenses or costs due to the return, destruction or deletion of personal data, these shall be borne by Controller.

10 Proof of Compliance with Data Protection Law

10.1 Upon request, Processor makes available to Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA.

10.2 In addition, Processor allows for and contributes to audits, including inspections, conducted by Controller or another auditor mandated by Controller or a supervisory authority. In particular, the Processor agrees that Controller or an auditor mandated by Processor is entitled, after giving reasonable advance notice, to on-site check the compliance with the provisions on data protection and the contractual agreements of this DPA provided that such on-site inspections will be conducted to the extent necessary during normal business hours of Processor and without disrupting Processor's operations.

10.3 If the auditor mandated by Controller is a competitor of Processor, Processor is entitled to raise an objection against this auditor.

10.4 Controller shall reimburse Processor for all expenses and costs incurred by Processor in carrying out and supporting an audit or inspection. Processor is not obliged to spend more than one (1) employee and working day per calendar year for such audits or inspections.

11 Records of Processing Activities

Processor shall maintain a record of processing activities in accordance with Art. 30 par. 2 GDPR and shall hand over the record to the supervisory authority upon request.

12 Other Obligations of Processor

12.1 Upon request, Processor shall cooperate with the supervisory authority when the latter is being performing its duties.

12.2 Processor has designated as data protection officer

Mr. Thomas Köhler, TeamSec GmbH, Batschkastraße 18, 67117 Limburgerhof, datenschutz@cognigy.com.

Processor shall notify Controller without undue delay and in writing of any change of the data protection officer.

12.3 If a data protection impact assessment is required for a planned processing of personal data, Processor shall assist Controller in the assessment upon request and against payment of the associated costs and shall provide Controller with all necessary documentation and relevant information.

12.4 Processor shall without undue delay inform Controller about control actions and measures of the supervisory authority according to Art. 58 GDPR as well as about investigations carried out by a competent authority according to Art. 83 GDPR and sections 42, 43 BDSG at Processor, as far as these control actions, measures or investigations relate to the order processing.

13 Infringements to be Notified

13.1 Processor shall without undue notify Controller if Processor becomes aware of any violation of the protection of personal data. Notifications shall be made in text form and shall include at least the information listed in Art. 33 par. 3 GDPR.

13.2 Processor is aware that, pursuant to Art. 33 and 34 GDPR, there may be obligations to notify the supervisory authority and the persons concerned in the event of a violation of the protection of personal data. Therefore, such incidents must be reported without undue delay to Controller, regardless of their cause. Processor shall, in consultation with Controller, take appropriate measures to secure the data and to mitigate possible adverse consequences for data subjects.

13.3 To the extent, Controller is subject to obligations pursuant to Art. 33 and 34 GDPR, Processor shall support Controller in this respect against payment of the costs incurred by Processor. Without limiting the foregoing, Controller remains responsible for fulfilling the notification and communication obligations pursuant to Art. 33 and 34 GDPR.

14 Appendices

The following appendices form an integral part of this DPA and shall prevail, in any case of conflict or uncertainties, the provisions the present DPA:

Appendix 1: Technical and Organisational Measures

Appendix 2: Sub-processors

Appendix 1: Technical and Organisational Measures

Office Düsseldorf

1 Pseudonymiszation and Encryption of Personal Data

1.1 Aim: Unauthorized persons shall be impeded or prevented from assigning personal data to an identifiable person.

1.2 Technical and organizational measures in place:

- Storage - encrypted data storage (only the strongest types of generally accepted, non-proprietary encryption algorithms are allowed, such as AES)
- Transmission - encrypted data transmission (e-mail encryption according to specific arrangement with addressee, encrypted Internet connections using TLS/SSL)

2 Access Control to Premises and Facilities

2.1 Aim: Unauthorised persons shall be prevented from gaining physical access to premises, buildings or rooms, where data processing systems are located which process personal data; persons are unauthorised if their activity does not correspond to tasks assigned to them. Exceptions may be granted for the purpose of auditing the facilities to third party auditors as long as they are supervised by the Processor and do not get access to the personal data itself.

2.2 Technical and organizational measures in place:

- visitor logging - logging of visitors (visitor book)
- Motion detector - motion detector
- Chip cards - chip card/transponder locking system
- Reception - visitor control at reception
- Manual locking system - manual locking system with locking cylinder
- Locking system - use of a locking system
- Video surveillance -video surveillance of the entrances

3 Access Control to Systems

3.1 Aim: Data processing systems must be prevented from being used without authorization.

3.2 Technical and organizational measures in place:

- authentication with user and password - authentication with user and password
- User authorizations - manage user authorizations (when entering, changing, leaving)
- Firewall - use of firewalls to protect the network
- MDM - use of Mobile Device Management
- Careful selection of personnel - careful selection of cleaning and security personnel
- Blocking external interfaces - content filter and intrusion detection for Zywall
- Encryption of data carriers - encryption of data carriers using state-of-the-art methods

4 Access Control to Data

4.1 Aim: Persons entitled to use a data processing system shall gain access only to the data to which they have a right of access, and personal data must not be read, copied, modified or removed without authorization in the course of processing.

4.2 Technical and organizational measures in place:

- Authorization concept - creation and implementation of an authorization concept
- Data deletion - Secure deletion of data media before reuse (e.g. by multiple overwriting)
- Use of document shredders - use of document shredders (min. security level 3 and protection class 2)

- Use of service providers - use of service providers for document and data destruction (if possible with DIN 66399 certificate)
- Password policy - password policy including length, complexity and frequency of change
- Secure storage - secure storage of data media
- Encryption of data carriers - encryption of data carriers using state-of-the-art methods

5 Disclosure control

5.1 Aim: Except as necessary for the provision of the services in accordance with the Main Contract personal data must not be read, copied, modified or removed without authorization during transfer or storage and it shall be possible to verify to whom personal data was transferred to.

5.2 Technical and organizational measures in place:

- Email encryption - email encryption using S/MIME or PGP (or other state of the art)
- SSL / TLS encryption - use of SSL/TLS encryption for data transmission on the Internet
- VPN tunnels - installation of VPN tunnels for dial-in into the network from outside

6 Input Control

6.1 Aim: It shall be possible to examine and establish retrospectively whether and by whom personal data have been entered into data processing systems, modified or removed.

6.2 Technical and organizational measures in place:

- Personalised user names - traceability of entry, modification and deletion of data through individual user names (not user groups)
- Logging - logging of data entry, modification and deletion
- Access rights - personalized access rights for traceability of access

7 Job Control

7.1 Aim: Personal data being processed on commission shall be processed solely in accordance with the Main Contract and related instructions of Controller. Processor shall perform the services and, in particular, the data processing services for personal data only in accordance with Controller's instructions.

7.2 Technical and organizational measures in place:

- Audits - regular data protection audits by the company data protection officer
- Selection - selection of the contractor under due diligence aspects (especially with regard to data security)
- AV contract - conclusion of an agreement on order processing in accordance with Art. 28 GDPR.
- DPO - appointment of a data protection officer
- Ongoing review - ongoing review of the contractor and its activities
- Training - training of all employees with access rights. Regularly taking place follow-up trainings
- Obligation - obligation to confidentiality in accordance with Art. 28 par. 3 s. 2 lit. b, 29, 32 par. 4 GDPR

8 Availability Control

8.1 Aim: Personal data shall be protected against disclosure, accidental or unauthorized destruction or loss.

8.2 Technical and organizational measures in place:

- Antivirus software - use of antivirus software to protect against malware
- Off-site data protection - keeping data protection in a secure, off-site location
- Backup & recovery concept - creation of a backup & recovery concept
- Fire alarm systems - fire and smoke detection systems
- Fire fighting equipment - CO2 fire fighting equipment in server rooms
- IT emergency plan - creation and application of IT emergency and recovery plans
- Air conditioning - air conditioning in server rooms
- Redundant data storage - redundant data storage (cloud systems like box.com for file storage)

- Protective socket strips - protective socket strips in server rooms
- Temperature monitoring - devices for monitoring temperature and humidity in server rooms
- Uninterruptible power supply - (UPS) uninterruptible power supply for server room equipment

9 Segregation Control

9.1 Aim: Personal data collected for different purposes shall be processed separately.

9.2 Technical and organizational measures in place:

- Logical client separation - logical client separation (software-side)
- Production and test system - separation of production and test system

10 Process for Regular Testing

10.1 Aim: A process must be implemented for regularly testing, assessing and evaluating of the effectiveness of technical and organizational measures taken by Processor to ensure the security of the processing.

10.2 Technical and organizational measures in place:

- Audits - conducting regular internal audits
- Incident response system - incident response system for the traceability of security breaches and problems
- Vulnerability analyses - implementation of regular IT vulnerability analyses (e.g. penetration test)
- Software presettings - use of software with data-protection-friendly pre-settings in accordance with (Art. 25 par. 2 GDPR)
- Software-supported tools - use of software-supported tools for compliance with data protection requirements (audatis MANAGER)

Data Center

1 Pseudonymiszation and Encryption of Personal Data

1.1 Aim: Unauthorized persons shall be impeded or prevented from assigning personal data to an identifiable person.

1.2 Technical and organizational measures in place:

- Storage - encrypted data storage (e.g. file encryption according to AES256 standard)
- Transmission - encrypted data transmission (encrypted Internet connections using TLS/SSL)

2 Access Control to Premises and Facilities

2.1 Aim: Unauthorised persons shall be prevented from gaining physical access to premises, buildings or rooms, where data processing systems are located which process personal data; persons are unauthorised if their activity does not correspond to tasks assigned to them. Exceptions may be granted for the purpose of auditing the facilities to third party auditors as long as they are supervised by the Processor and do not get access to the personal data itself.

2.2 Technical and organizational measures in place:

- visitor logging - logging of visitors (visitor book)
- Chip cards - chip card/transponder locking system
- Reception - visitor control at reception
- Manual locking system - manual locking system with locking cylinder
- Doorman – general identity check at the doorman
- Locking system - use of a locking system
- Video surveillance -video surveillance of the entrances

3 Access Control to Systems

3.1 Aim: Data processing systems must be prevented from being used without authorization.

3.2 Technical and organizational measures in place:

- authentication with user and password - authentication with user and password
- User authorizations - manage user authorizations (when entering, changing, leaving)
- Firewall - use of firewalls to protect the network
- MDM - use of Mobile Device Management
- Encryption of data carriers - encryption of data carriers using state-of-the-art methods

4 Access Control to Data

4.1 Aim: Persons entitled to use a data processing system shall gain access only to the data to which they have a right of access, and personal data must not be read, copied, modified or removed without authorization in the course of processing.

4.2 Technical and organizational measures in place:

- Authorization concept - creation and implementation of an authorization concept
- Data deletion - Secure deletion of data media before reuse (e.g. by multiple overwriting)
- Use of document shredders - use of document shredders (min. security level 3 and protection class 2)
- Use of service providers - use of service providers for document and data destruction (if possible with DIN 66399 certificate)
- Password policy - password policy including length, complexity and frequency of change
- Secure storage - secure storage of data media
- Encryption of data carriers - encryption of data carriers using state-of-the-art methods

5 Disclosure control

5.1 Aim: Except as necessary for the provision of the services in accordance with the Main Contract personal data must not be read, copied, modified or removed without authorization during transfer or storage and it shall be possible to verify to whom personal data was transferred to.

5.2 Technical and organizational measures in place:

- Email encryption - email encryption using S/MIME or PGP (or other state of the art) in selected situations
- SSL / TLS encryption - use of SSL/TLS encryption for data transmission on the Internet
- VPN tunnels - installation of VPN tunnels for dial-in into the network from outside

6 Input Control

6.1 Aim: It shall be possible to examine and establish retrospectively whether and by whom personal data have been entered into data processing systems, modified or removed.

6.2 Technical and organizational measures in place:

- Personalised user names - traceability of entry, modification and deletion of data through individual user names (not user groups)
- Logging - logging of data entry, modification and deletion
- Access rights - personalized access rights for traceability of access

7 Job Control

7.1 Aim: Personal data being processed on commission shall be processed solely in accordance with the Main Contract and related instructions of Controller. Processor shall perform the services and, in particular, the data processing services for personal data only in accordance with Controller's instructions.

7.2 Technical and organizational measures in place:

- Audits - regular data protection audits by the company data protection officer
- Selection - selection of the contractor under due diligence aspects (especially with regard to data security)
- DPA - conclusion of an agreement on order processing in accordance with Art. 28 GDPR.

- DPO - appointment of a data protection officer
- Ongoing review - ongoing review of the contractor and its activities
- Training - training of all employees with access rights. Regularly taking place follow-up trainings
- Obligation - obligation to confidentiality in accordance with Art. 28 par. 3 s. 2 lit. b, 29, 32 par. 4 GDPR

8 Availability Control

8.1 Aim: Personal data shall be protected against disclosure, accidental or unauthorized destruction or loss.

8.2 Technical and organizational measures in place:

- Antivirus software - use of antivirus software to protect against malware
- Off-site data protection - keeping data protection in a secure, off-site location
- Backup & recovery concept - creation of a backup & recovery concept
- Fire alarm systems - fire and smoke detection systems
- Fire fighting equipment - CO2 fire fighting equipment in server rooms
- IT emergency plan - creation and application of IT emergency and recovery plans as part of the SOC2 certification
- Air conditioning - air conditioning in server rooms
- Redundant data storage - redundant data storage (e.g. mirrored hard drives, RAID 1 or higher, mirrored server room)
- Protective socket strips - protective socket strips in server rooms
- Temperature monitoring - devices for monitoring temperature and humidity in server rooms
- Uninterruptible power supply - (UPS) uninterruptible power supply

9 Segregation Control

9.1 Aim: Personal data collected for different purposes shall be processed separately.

9.2 Technical and organizational measures in place:

- Logical client separation - logical client separation (software-side)
- Production and test system - separation of production and test system

10 Process for Regular Testing

10.1 Aim: A process must be implemented for regularly testing, assessing and evaluating of the effectiveness of technical and organizational measures taken by Processor to ensure the security of the processing.

10.2 Technical and organizational measures in place:

- Audits - conducting regular internal audits
- Incident response system - incident response system for the traceability of security breaches and problems
- Management system for data protection - management system for data protection
- Management system information security - management system for information security
- Vulnerability analyses - implementation of regular IT vulnerability analyses (e.g. penetration test)
- Software presettings - use of software with data-protection-friendly pre-settings in accordance with (Art. 25 par. 2 GDPR)
- Software-supported tools - use of software-supported tools for compliance with data protection requirements (audatis MANAGER)

B. Amazon Web Services

The technical and organizational measures applicable to Amazon Web Services valid at the time of entering into this Data Processing Agreement can be found in AWS' DPA (AWS GDPR Data Protection Addendum) at https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

C. Microsoft

The technical and organizational measures applicable to Microsoft 365 valid at the time of entering into this Data Processing Agreement are set forth in Microsoft's DPA (Data Protection Addendum) at. https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14

Appendix 2: Sub-processors

Name / company, address	Job Description	Scope of Order Processing
AWS Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855 Luxembourg	Scalable infrastructure	Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides customizable computing capacity in the cloud. The service is designed to facilitate cloud computing for developers.
Microsoft Ireland Operations Limited, 1 Microsoft Place, South County Business Park, Leopardstown Dublin 18, Ireland	Scalable infrastructure	Applications are built, managed, and deployed across a large global network using preferred tools and frame-works, project management.
Audiocodes Ltd. 1 Hayarden Street, Airport City, Lod 7019900, Ben Gurion Airport, Israel 7019900	Voice Gateway Managed Service	Provision of Voice Gateway Managed Service, maintenance, monitoring and operation of Voice Gateway infrastructures on Cognigy or customer infrastructure.