Data processing Agreement (AV contract)

pursuant to Article 28 (3) of the EU General Data Protection Regulation (EU GDPR)

11.01.2022

between the client and Copexa GmbH (Wagnerstraße 25, 76448 Durmersheim, Germany) as processor / contractor.

PREAMBLE

The processing is based on the contract between the parties for the provision of various services by the contractor (main contract).

§1 Subject of the agreement

1. The contractor collects / processes / uses personal data on behalf of the client.

2. Subject of the contract

The purpose of the contract is to process data by collecting, inquiring, organizing, sorting, storing, adapting or modifying, reading, querying, using, disclosing through transmission, dissemination or any other form of provision, matching or linking, restriction, erasure or destruction of data exclusively in connection with the services listed in the main contract. In particular, this involves the provision of a platform that enables the client to conduct surveys of third parties or to obtain and evaluate third-party evaluations. It will address data of the client among others used to send the surveys by e-mail. Processing for other purposes does not take place.

The contractual services are provided by the contractor himself exclusively in member states of the EU or in a state party to the Agreement on the European Economic Area. A transfer of the services or partial work to a third country may only take place if the special requirements of Art. 44 et seq. DSGVO are fulfilled and this is absolutely necessary for the provision of the services.

Changes to the processing object and procedural changes must be agreed together.

3. Duration of the contract

The contract begins with the signature of both parties and ends with the effectiveness of the termination of the main contract.

4. Scope, nature and purpose of data collection, processing or use

4.1 Type of processing

The contractor processes personal data of customers, employees, business contacts and interested parties of the client.

4.2 Type of personal data

Personal data required for the execution of the service are personal master data (especially name) and communication data (especially e-mail address).

4.3 circle of those affected
– Customers and employees
– Business contacts and prospects

§2 Rights and obligations of the client

1. The client alone is responsible for the assessment of the admissibility of data collection / processing / use and for the protection of the rights of the persons concerned.

2. The client issues all orders or partial orders in writing or in a documented electronic format.

3. The client has the right to issue written instructions to the contractor with regard to the processing of personal data provided to him.

4. The client is entitled to convince himself of the compliance with the technical and organizational measures taken at the contractor, as well as the obligations arising from this contract prior to the start of data processing and then regularly. The client can also have this check carried out by a third party. The client undertakes to remunerate the expenses incurred by the contractor within the framework of making inspections possible.

5. The client informs the contractor immediately if he finds any errors or irregularities in the examination of the order results.

6. The client is obliged to treat confidentially all acquired knowledge of business secrets and data security measures of the contractor within the framework of the contractual relationship. This obligation remains valid even after termination of this contract.

§3 Duties of the contractor

1. The contractor processes personal data exclusively in accordance with the agreements made, the legal basis and instructions of the client in accordance with the GDPR, unless he is obliged to process by the law of the European Union or of the member state to which the processor is

subject (eg Investigations of law enforcement and state protection authorities). If this is the case, the processor must notify the controller of these legal requirements before processing, unless such communication is prohibited by the law in question for important public interest (Article 28 (3) (2) (a) GDPR).

2. The contractor shall correct, delete and block personal data from the contractual relationship or limit its processing if the client requests so in the agreement or an instruction and does not oppose the legitimate interests of the contractor. Insofar as an affected person directly addresses the contractor in this regard, the contractor will immediately forward this request to the client. The contractor is entitled to make corresponding changes himself, if the client does not react to corresponding inquiries of the persons concerned. The client undertakes to remunerate the expenses incurred by the contractor.

3. The contractor does not use the personal data provided for data processing for any other, especially not for own purposes. Copies or duplicates are not created without the knowledge of the client. The contractor assures the contractual processing of all agreed measures in the area of orderbased processing of personal data. He assures that the processed data is strictly separated from other data.

4. The contractor will immediately inform the client if, in his opinion, an instruction issued by the client violates statutory provisions. The Contractor shall be entitled to suspend the execution of the relevant instruction until it has been confirmed or changed by the person responsible at the Client.

5. The contractor agrees that the client - by appointment - is entitled to control compliance with this agreement to the extent required under Art. 28 DSGVO itself or by third parties commissioned by the client. The contractor undertakes to provide the client with the necessary information and to prove the implementation of the technical and organizational measures. The client undertakes to remunerate the expenses incurred by the contractor within the framework of making inspections possible.

6. After completion of the contractual work, the contractor must have all data, documents and processing or utilization results created in connection with the order relationship deleted or destroyed or destroyed in accordance with the order, unless this is a legal requirement or actual reason.

7. The contractor confirms that he is familiar with the data protection regulations of the DSGVO that are relevant to the processing of order data and that he complies with his respective obligations.

8. The contractor undertakes to maintain confidentiality in the processing of the client's personal data. This will continue after the end of the contract.

9. The contractor warrants that he acquaints the employees involved in the execution of the work with the provisions of data protection that are relevant to them and that he commits them to secrecy, both during their employment and after their employment. The contractor monitors compliance with the data protection regulations specified here in his company.

10. The contractor may only provide information about personal data from the contractual relationship to third parties or the data subject with the prior instruction or written consent of the client, or insofar as this information is provided on the basis of legal obligations.

§4 subcontractors

1. The client agrees to the commissioning of subcontractors for the processing of data by the contractor. The approval required under Art. 28 (2) and (9) GDPR is hereby granted.

2. The contractor shall ensure that he has carefully selected the subcontractor with special consideration of the suitability of the technical and organizational measures taken by him within the meaning of Art. 32 DSGVO.

3. Subcontractors in third countries may only be commissioned if the special conditions of Art. 44 et seq. GDPR are fulfilled (for example Commission adequacy decision, standard data protection clauses, approved codes of conduct) or if their commissioning is absolutely necessary for the provision of the service by the contractor.

4. The contractor must ensure that the agreed regulations between the client and the contractor apply as far as possible to subcontractors and will regularly check compliance with the obligations of the subcontractor(s).

5. In the contract with the subcontractor, the details shall be specified so that the responsibilities of the contractor and the subcontractor are clearly distinguished from each other. If several subcontractors are used, this also applies to the responsibilities between these subcontractors.

6. The subcontractors currently engaged in the processing of personal data for the contractor are listed in the respective service description or derive from the service offered. The client agrees to their commissioning.

7. The processor shall notify the controller in advance of any change in

relation to the incorporation of new or the replacement of existing subcontractors, giving the client the opportunity to object to such changes (Article 28 (2) sentence 2 GDPR).

§5 Technical and organizational measures

1. The contractor shall guarantee an appropriate level of protection for the specific data processing of the risk for the rights and freedoms of natural persons affected by the processing. This shall take into account at least the protection objectives of confidentiality, availability and integrity of the systems and services, as well as their resilience in terms of the nature, extent, circumstances and purpose of the processing so as to reduce the risk permanently by appropriate technical and organizational corrective measures.

2. The data protection concept used by the contractor has implemented its technical and organizational measures, taking into account the state-of-the-art protection goals and taking particular account of the IT systems and processing processes employed by the contractor.

3. The contractor complies with the principles of proper data processing. It ensures the contractually agreed and legally prescribed data security measures.

4. The technical and organizational measures may be adapted to the technical and organizational development in the course of the contractual relationship. The contractor shall establish procedures for the periodic review, evaluation and evaluation of the effectiveness of the measures taken to ensure the safety of the processing. Significant changes will be communicated to the client in documented form.

5. The contractor shall immediately notify the client of any disruptions, violations by the contractor or persons employed by him against data protection regulations or the stipulations made in the order, as well as the suspicion of data breaches or irregularities in the processing of personal data. This applies above all with regard to any notification and notification obligations of the client according to Art. 33 and 34 DSGVO. The contractor warrants to support the client adequately in his duties under Art. 33 and 34 DSGVO.

§6 liability

1. The customer is responsible to the person concerned for compensation for damages suffered by a data subject as a result of data processing that is inadmissible or incorrect for data protection within the scope of the contractual relationship. The contractor's recourse to such damage by

third parties to the contractor is only permissible if the contractor has grossly negligently or deliberately violated this contract.

2. Otherwise, the liability regulations for the individual services of the contractor in the main contract have been agreed.

§7 special right of termination

1. In the case of serious violations of the provisions of this contract, in particular against compliance with applicable data protection regulations, the client is granted a special right of termination. Further sanctions, in particular contractual penalties are excluded.

2. A serious breach shall, in particular, exist if the contractor has not materially fulfilled or has not fulfilled the obligations specified in this agreement.

3. In the case of insignificant infringements, the client shall set a reasonable deadline for the contractor to remedy the situation. If the remedy does not occur in time, the client is entitled to extraordinary termination as described in this section.

§8 Miscellaneous

1. Both parties are obliged to treat confidentially all knowledge of trade secrets and data security measures of the respective other party gained in the context of the contractual relationship, even beyond the termination of the contract. If there are any doubts as to whether the information is subject to confidentiality, it must be treated as confidential until written approval by the other party.

2. The written form is required for side agreements.

3. Terms used in this contract are to be understood according to their definitions in the EU General Data Protection Regulation.

4. Both texts of the AV contract in German and English are binding, in case of doubt the German version applies.

§9 Effectiveness of the agreement

Should individual parts of the agreement be ineffective or unenforceable, this does not affect the validity of the agreement otherwise. The invalid or unenforceable provision shall be replaced by an effective and enforceable provision whose effectiveness comes closest to the economic objective pursued by the parties with the invalid or unenforceable provision processing / use and for the protection of the rights of the persons concerned.

Appendix I to the AV contract

Technical and organizational measures at the Order data processing

1. Subject matter of the contract

The order of the client to the contractor includes the following work and / or services:
[X] Personal data [] Sensitive data (cf. Art. 9 GDPR)

The contractor provides the following services for the client:
[X] Customer surveys

Data processing affects employees, customers, suppliers and interested parties of the client.

2. Authorized to receive instructions

Persons of the contractor who are authorized to receive instructions are:
1. Markus Kölmel

3. Technical and organizational measures

1. Entry Control
   Unauthorized access is to be prevented, whereby the term is to be understood spatially. Technical or organizational measures for access control, in particular also for the legitimation of authorized persons:
   - External barrier
   - Alarm system
   - Video surveillance (inside / outside)
   - Manual locking system
   - Security locks
   - Doors with outside knobs
   - Care in choosing cleaning services

2. Admission Control
   The intrusion of unauthorized persons into the IT systems must be prevented. Technical (password / password protection) and organizational (user master record) measures with regard to user identification and authentication:
   - The server systems are password-protected against unauthorized use and access.
   - Login with username + password
   - Anti-virus software clients
   - Firewall
   - Intrusion detection systems
   - Housing lock

- BIOS protection (separate password)
- Blocking of external interfaces (USB)
- Automatic desktop lock
- Manage user permissions
- Creation of user profiles
- Central password assignment
- General data protection guidelines and / or safety
- Maintenance access via the network takes place via SSH via an encrypted connection using a user name and password or private keys.
- Access to the backup system via SSH connection with user name and private key.
- There is a password policy for the passwords
- Passwords for customer systems are only known to a small group of administrators.

3. User Access Control

   Unauthorized activities in IT systems outside of the granted authorizations must be prevented. Demand-oriented design of the authorization concept and the access rights as well as their monitoring and logging:

   - Access via username and password or private keys
   - Restriction of access rights to necessary systems
   - Logging of administrative access
   - The client's administrative access is restricted
   - The backup system is also protected against unauthorized access by a firewall.
   - The use of the backup system, including the functions performed, is logged together with the user name.
   - Document shredders

4. Transfer Control

   Aspects of the transfer of personal data are to be regulated. Measures for transport, transfer and transmission or storage on data carriers (manual or electronic) as well as for subsequent verification:

   - The administration data is only transmitted in encrypted form (SSH)
   - The data is only transferred to the backup system via an encrypted connection.
   - There is an internal company regulation for administrative remote access.
   - The backup system logs who accesses, deletes or backs up which files and when.
   - Email encryption
   - Provision via encrypted
   - Connections such as sftp, https

5. Input Control

   The traceability and documentation of the data administration and maintenance must be guaranteed. Measures to subsequently check whether and by whom data has been entered, changed or removed (deleted):

- Technical logging of the entry, modification and deletion of data
- Manual or automated control of the logs
- Traceability of input, change and deletion of data through individual user names (not user groups)
- Storage of forms from which data is automatically processed edits were taken over

6. Order control

   The order data processing in accordance with the instructions must be guaranteed. Measures (technical / organizational) to delimit the competencies between client and contractor:

   - Contractual regulations
   - Orders must be placed in writing (email is sufficient)
   - Documentation of all orders with result / reporting
   - Regular control of the contractor (subcontractor)
   - Selection of contractors (subcontractors) taking into account the requirements of the GDPR)

7. Separation Control

   Data collected for different purposes must also be processed separately. Measures for the separate processing (storage, modification, deletion, transmission) of data with different purposes:

   - Presence of procedural documentation
   - Implementation of programming rules
   - Regulations for system and program audits
   - Logical separation of data sets
   - Internal multi-tenancy
   - Separate test and production environment

8. Availability Check

   The data must be protected against accidental destruction or loss. Data backup measures (physical / logical):

   - Fire alarm system
   - Monitoring of the ambient conditions (temperature, humidity, etc.).

Appendix II to the AV contract

List of existing subcontractors at the time the contract was concluded

1. **Data center & server management:**

   netcup GmbH
   Daimlerstraße 25
   DE-76185 Karlsruhe
   E-Mail: mail@netcup.de

2. **Email provider**:

   EUNETIC GmbH
   Wagnerstr. 25
   DE-76448 Durmersheim
   E-Mail: info@eunetic.com

   SparkPost, a MessageBird company
   9160 Guilford Rd
   Columbia, MD 21046
   E-Mail: privacy@sparkpost.com