Data Processing Agreement
Article 28 GDPR

Agreement

between

the Partner of the main agreement

– Controller, hereinafter referred to as “the Principal” –

and

Good Conversations gGmbH

Buceriusstraße, Eingang Speersort 1, 22095 Hamburg

– Processor, hereinafter referred to as “the Agent” –

Principal and Agent individually designated as “Party” and collectively as “Parties”.

1. Subject-matter

In the framework of the delivery and performance relationship between the parties (hereinafter referred to as the “Main Agreement”) it is necessary that the Agent handles personal data as a processor in the sense of Article 4 no. 8 GDPR, for which the Principal is responsible as controller in the sense of Article 4 no. 7 GDPR (hereinafter referred to as “Principal-Data”). This Agreement concretizes the data privacy rights and duties of the parties in the context of handling the Principal-Data for the performance of the Main Agreement by the Agent.

2. Nature and purpose of the processing, nature of the personal data, categories of data subjects, duration of the processing

The Agent shall process the Principal-Data for the duration of the contract on behalf of and in compliance with the instructions of the Principal. The Principal remains the controller according to Article 5 (2) GDPR ("Master of the Data "). Nature and purpose of the processing as well as the nature of the personal data and the categories of data subjects are specified in **Annex 1**. The Agent shall not process any personal data deviating from or going beyond this, in particular if its for the Agents’ own purposes.

3. Principal’s rights to give instructions

3.1 Instructions from the Principal shall be given in writing or text form (e-mail being sufficient). Deviating from this, (telephone) verbal instructions may be given, if they are subsequently confirmed in writing or text form.

3.2 The Agent shall carry out the instructions of the Principal without undue delay or, where applicable, in compliance with a reasonable deadline set by the Principal. The agent shall, in particular, rectify, delete and block personal data as instructed by the Principal without undue delay and confirm this in writing upon request.

3.3 If the Agent considers that an admissible individual instruction violates applicable provisions of the General Data Protection Regulation or other data privacy provisions of EU law or the law of the Member States, he shall point this out to the Principal without undue delay. The Agent is entitled to suspend the execution of the instruction until the instruction is confirmed by the Principal.

3.4 Insofar as the Agent is required to process the personal data without any instruction from the Principal by Union or Member State law to which the Agent is subject, the Agent shall inform the Principal of that legal requirement in due time before processing, unless that law prohibits such information on important grounds of public interest.

4. Duties of the Principal

4.1 The Principal shall be externally, i. e. vis-à-vis third parties and data subjects, responsible for the lawfulness of the processing of the Principal-Data and for safeguarding the rights of data subjects.

4.2 The Principal shall keep all business secrets of the Agent (in particular those with regard to technical and organisational measures) acquired in the context of the contractual relationship confidential. This obligation shall remain in force even after termination of this contract.

4.3 Insofar as the Agent defends himself with legal means against a claim for damages according to Article 82 GDPR, against an imminent or already imposed administrative fine according to Article 83 GDPR or other sanctions in the sense of Article 84 GDPR, the Principal shall allow the Agent to disclose details of the processing for the purpose of legal defense, including instructions issued from the Principal.

4.4 The Principal shall support the Agent in the case of controls by a supervisory Authority, regulatory offence procedures, criminal procedures, claims to compensation or liability of the data subject or a third person in a reasonable and necessary manner, as far as these controls concern the data processing by the Agent.

5. Duties of the Agent

5.1 If a data subject addresses the Agent directly in the exercise of his rights under Chapter 3 GDPR (Art. 12-23 GDPR), taking into account Part 2, Chapter 2 BDSG (Sections 32-37 BDSG), the Agent shall immediately forward this request to the Principal and support the Principal in a reasonable manner with appropriate technical and organisational measures to comply with his obligation to respond to such requests for the exercise of the rights of the data subject specified in Chapter 3 DSGVO.

5.2 The Agent shall support the Principal in complying with the duties arising out of Art. 32-36 GDPR taking into account the nature of the processor and the information available to the Agent.

5.3 If the Agent becomes aware of a personal data breach within the meaning of Art. 4 No. 12 GDPR it shall immediately notify the Principal thereof. Within this notification pursuant to Art. 33 para. 2 DSGVO, the Agent shall inform the Principal as comprehensive as possible about the

nature and extent of the incident and the time it occurred, the IT system and data subjects affected, the time of discovery, all conceivable adverse consequences of the personal data breach and the measures taken as a result.

5.4 The Agent informs the Principal without undue delay if the rights of the Principal concerning the personal data held by the Agent are significantly affected by measures taken by third parties or other events.

5.5 The Agent shall return all Principal-Data at the request of the Principal. Data carriers received from the Principal shall be marked separately and administered on an ongoing basis. Copies and duplicates of the personal data may only be made with the prior consent of the Principal, unless they are used for the proper execution of this agreement or the respective project assignment or to comply with legal storage obligations.

5.6 If the Agent is legally required, it shall assign a data protection officer (Art. 37-39 GDPR). His or her contact details and where applicable information about his or her replacement shall be given to the Principal for the purpose of direct contact at least in text form (e-mail being sufficient).

6. Security in the processing

6.1 The Agent shall take all measures necessary pursuant to Art. 32 GDPR to grant a level of data security commensurate with the risk of processing. In particular, these measures include the ability to restore the confidentiality, the integrity, the availability and the resilience of the systems permanently and to restore the availability of and access to personal data quickly after a physical or technical incident. The Agent shall regularly review, assess and evaluate the effectiveness of the technical and organisational measures taken to grant the security of the processing and documents the results.

6.2 The Agent shall implement the technical and organisational measures listed in **Appendix 2** prior to commencing the processing of Principal-Data, to maintain them for the duration of the processing and to adapt them commensurate with the state of the art and the risk of the processing.

6.3 The Agent shall ensure that all persons authorized to process personal data are obliged to confidentiality or are subject to an adequate statutory confidentiality obligation.

7. Supervision authority of the Principal

7.1 The Agent shall grant the Principal the right to evaluate the data processing and the compliance with this contract or the respective project assignment. In particular, the Agent shall provide the Principal with all information required to prove compliance with the obligations laid down in this Agreement and shall enable the execution of evaluations, including inspections. These actions may also be carried out by a third party obliged to confidentiality, provided that the third party is not a competitor of the Agent.

7.2 The parties agree that the Principal shall conduct an evaluation in accordance with Clause 7.1 by instructing the Agent, at the Agents' option, to submit an appropriate audit report, a report or extracts of reports from independent bodies (e.g. accountants, auditors, data protection officers, data protection officers, data protection auditors or quality auditors) or an appropriate certification by an IT security or data protection audit - e.g. in accordance with ISO/IEC 27001 or

“BSI-Grundschutz” (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI)) - ("Audit Report"). Notwithstanding, the Principal may conduct an independent evaluation when reasonably justified.

7.3 The Agent shall support the Principal in its evaluation. This includes granting the Principal all access, information and inspections rights. The same applies to evaluations conducted by the competent supervisory authority in accordance with the applicable data protection regulations.

7.4 The Principal shall inform the Agent about all circumstances relating to the conduct of the evaluation in due time (generally at least four weeks prior to the evaluation). Generally, the Principal may conduct an evaluation once per calendar year. Notwithstanding the foregoing, the Principal shall have the right to conduct further evaluations in the event of special occurrences.

8. Subprocessors

8.1 The Agent may subcontract with further processors (subprocessors). For the time being, the Agent commissions the subcontractors listed in Appendix 3. The Principal agrees to their commissioning. The Agent shall always inform the Principal of any intended change in relation to the use or replacement of subcontractors, which shall give the Principal the opportunity to object to such changes within two weeks, although this may not be done without good cause in terms of data protection law. Unless the Principal raises justified objections within two weeks of notification of the change, the change shall be deemed to have been approved by the Principal. The Agent shall inform the Principal of this significance of his conduct at the beginning of the period. In the event of an objection, the Agent may, at his own discretion, either provide the service without the intended change or - if the provision of the service without the intended change is not reasonable for the Agent - discontinue the service to the Principal within two weeks of receipt of the objection and terminate the main contract without notice and with immediate effect.

8.2 Should the commissioning of a subprocessor lead to a transfer of Principal-Data to a country outside of the European Union (EU) or the European Economic Area (EEA) (‘third country’), clause 9 of this agreement applies.

8.3 The Agent shall ensure that the data protection obligations stipulated in this Agreement also apply vis-à-vis the subcontractor. The Agent shall oblige the subprocessor respectively pursuant to Art. 28 (4) GDPR by way of a contract or another legal instrument in accordance with EU law or the law of the respective member state prior to the commencement of the processing, whereby, in particular, sufficient guarantees must be provided that the appropriate technical and organisational measures are conducted in such a way that the processing complies with the regulations of the GDPR.

9. Transfer of Principal-Data to third countries

9.1 Generally, the data processing contractually agreed upon shall be conducted in a member state of the European union (EU) in a signatory state of the Agreement on the European Economic Area (EEA). Any transfer of Principal-Data to a country outside the EU/EEA ("third country") shall only take place if the special requirements of Art. 44 et seq. GDPR are met.

9.2 The Principal hereby authorises the Agent to conclude the standard contractual clauses for the transfer of personal data to processors established in third countries in accordance with

Commission Decision 2010/87/EU of 5.2.2010, OJ 2010 L 39 on behalf of the Principal, with a subprocessor to whom the Agent intends to transfer data for processing in a third country.

10. Return and deletion

10.1 The Agent shall return all Principal-Data after having finished the processing agreed on and, in particular after the end of the contractual performance (in particular in the event of termination or other end of the Main Agreement) and subsequently delete this data in accordance with the applicable regulations (including existing copies). Data carriers obtained by the Principal shall be returned or destroyed in compliance with an appropriate level of protection. The same applies to test and rejection material. This shall not apply provided Union or Member State law requires storage of the personal data.

10.2 Documentations which serve the purpose of proving the orderly and due data processing or legal requirements of record-keeping shall be kept by the Agent according to the respective record-keeping periods beyond the duration of the contract.

11. Exemption

Insofar as claims for damages pursuant to Article 82 GDPR are made against the Agent for an infringement of the GDPR while processing of Principal-Data without the Agent having contravened a Principal's instruction, the Principal shall indemnify the Agent upon first request from all claims. The Principal shall also cover the costs of the Agent´s necessary legal defence including all court and legal fees. The obligation to indemnify shall not apply if the claim for damages is based on the violation of a duty under the GDPR specifically imposed on the processors such as the Agent.

12. Remuneration

The Agent may be compensated by the Principal for support services according to Clause 5.1 and Clause 5.2 of this agreements as well as for participation in independent inspections of the customer according to Clause 7.2 demand an appropriate remuneration. This shall not apply if the support is necessary because the Agent violates an instruction of the Principal or has violated an obligation from the GDPR specifically imposed on the processors.

13. Duration and termination

The term and termination of this Agreement shall be governed by the provisions concerning the term and termination of the Main Agreement. A termination of the Main Agreement automatically results in the termination of this Agreement. An isolated termination of this Agreement is excluded.

14. Priority clause

Unless special provisions are contained in this Agreement, the provisions of the Main Agreement shall apply. In the case of any conflicts between provisions of this Agreement and provisions of other agreements, in particular with the Main Agreement, the provisions of this Agreement shall prevail.

Appendix:

Appendix 1: Nature and purpose of the processing, Type of personal data, Categories of data subjects

Appendix 2: Technical and organisational matters

Appendix 3: Subcontractors

Appendix 1: Nature and purpose of the processing, Type of personal data, Categories of data subjects

Nature and purpose of the processing:

Hosting, service und support of the software platform My Country Talks

Type of personal data:

The following user data will be collected and used: answers to political questions given by participants during the application process, and personal data including name, gender, age, zip code, email address, and mobile phone number. Furthermore, anonymized data will be stored and used for statisticial evaluations and visualisations.

Categories of data subjects:

Customer data

Appendix 2: Technical and organisational measures

1. Confidentiality (Article 32 (1) Point b GDPR) and Encryption (Article 32 (1) Point a GDPR)

Physical Access Control

No unauthorised access to Data Processing Facilities:

ZEIT ONLINE

- Entrance doors are always kept locked
- Chip cards for all doors
- Visitors / external persons are accompanied or picked up and always supervised
- Video surveillance with recording at the front entrance
- Electronic door opener
- Security and / or security personnel at the entrance
- Alarm system
- Laptops locked away or lock to desks after work
- Fire doors, fire extinguishers, surge protection

diesdas.digital (development agency)

- Video surveillance outside working hours
- Security doors
- Office locked at any time, when no one is present
- Alarm system
- Window bars
- Laptops locked away after work in a cabinet
- Fire doors, fire extinguishers, surge protection

Makandra (Hosting)

- Access to the “aiti-park” (office building) is only possible with an anti-Park-ID. It is documented which card can open which door. All makandra employees have the same permissions
- The plant security officers regularly control all premises
- Access to the premises of the IT (server) is only possible for a limited group of people. Access to the server rooms is even more limited

Electronic Access Control/Encryption

No unauthorised use of the Data Processing and Data Storage Systems:

ZEIT ONLINE and diesdas.digital

- Standardized, documented process for managing user access
- cancellation / deactivation upon termination of the employment relationship
- regular review of all existing accounts and access
- granular allocation of access per service
- no external admins, service or maintenance
- Administration access for each service is kept to a minimum
- Admin access only for people who have excelled in the past as professionally and personally suitable
- No use of production data in local test systems
- Training for the handling of personal data and protection of the devices
- Routine encryption of all hard disks
- No sharing of computers: each employee has his own device and knows the access alone
- whenever possible data transmission through encrypted connections

Passwords

Using the password manager 1password mandatory for all employees;
Share visibility across multiple pools within the tool so that employees only can get passwords they need
1password allows the generation of secure passwords with minimum length and use of special characters;
Employees are required to use long passwords without repetitions and special characters
Instruction / training on 1password at the beginning of the employment relationship
Passwords must not be passed on; instructions for secrecy
At any time comprehensible which persons have access to which passwords
Former employees lose access to all passwords from the last working day

Makandra (Hosting)

An automatic lock occurs on computers within the domain
All computers within the domain are encrypted.
All employees are required to use randomly generated passwords and store them in an encrypted form

Internal Access Control

No unauthorised Reading, Copying, Changes or Deletions of Data within the system:

ZEIT ONLINE and diesdas.digital

Use of role and access rights management in all software products that make this possible
Restricting each person's access to data that is not necessary for their daily work
Use of granular role systems to restrict access to relevant and work-related data
Own passwords / access for each person; no account sharing
Regular control of assigned access rights by several persons
Access permissions are stored in the applications until the end of the employment relationship and can be viewed by the administrators at any time
If possible, purchase of software packages for access logging
SSH and SFTP if possible during data transmission
Encryption of the HTTP connection via TLS whenever possible
Encryption of all computers via FileVault
Deletion of files that are no longer needed, e.g . exports
Access from sensitive data only for as few people as possible
Passing on data through password-protected files if possible and communicating the access password only to recipients on a second channel
Initial meeting on data security, in which roles and access rights are defined
Analog data is destroyed with shredder of security level 4 with particle cut

Makandra (Hosting)

A role concept is used. In some cases roles are defined for individuals
Program-based authorizations are currently assigned individually

Isolation Control

The isolated Processing of Data, which is collected for differing purposes:

ZEIT ONLINE and diesdas.digital

Separation of access rules via database principle
Software-side client separation
Separation of productive and test systems (in separate databases)

Makandra (Hosting)
- All data is entered and processed separately only for the respective individual customers in the system. The data is stored separately for each customer according to his contract and his instructions

2. Integrity (Article 32 (1) Point b GDPR)

Data Transfer Control

No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport:

All systems accessible externally via the internet are only accessible via encrypted protocols
The company's security devices and encryption techniques apply to corporate devices issued to employees. In addition, a separate IT user policy applies

Data Entry Control

Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted:

Changes to data are logged system-internally.
In some cases, document-related logging of the logged-in user is implemented in other systems.
The file system records on an application level, who created or last edited a file
These protocols are evaluated only in acute individual cases

3. Availability and Resilience (Article 32 (1) Point b GDPR), Rapid Recovery (Article 32 (1) Point c GDPR)

Availability Control

Prevention of accidental or wilful destruction or loss

There is a backup concept in use and an emergency plan available
A procedure is defined for an information security incident

4. Procedures for regular testing, assessment and evaluation (Article 32 (1) Point d GDPR; Article 25 (1) GDPR)

Order or Contract Control

No third party data processing as per Article 28 GDPR without corresponding instructions from the Client:

Agents are carefully selected
Clear and unambiguous contractual arrangements
Formalised Instructions Management
Instructions are issued in writing
Strict controls of the Agent by the management or the data protection officer
duty of pre-evaluation

Makandra (Hosting)
Regular internal audits and other measures
Processing of personal data of the customer on his behalf only on the basis of a contract for the processing of orders according to Art. 28 General Data Protection Regulation