Data Processing Agreement

Agreement on the Processing of Personal Data pursuant to Article 28 General Data Protection Regulation (GDPR)

§ 1 Subject matter of the Agreement

(1) In the context of the performance of the contract between Wonder Technologies GmbH, Tempelhofer Ufer 1A, 10961 Berlin, Germany (hereinafter referred to as "Processor") and the contracting party (hereinafter referred to as "Controller"), jointly also referred to as "The Parties", the Processor processes personal data within the meaning of Article 4 No. 1 GDPR for the Controller (hereinafter referred to as "controller data") exclusively on behalf of and in accordance with the instructions of the Controller.

(2) The Processor shall process any controller data solely within the scope to provide video interface and the wonder.me platform to the end customer as determined in Appendix 1 and on behalf and in accordance with the instructions of the Controller. The Controller shall be solely responsible for assessing the lawfulness of the data processing.

(3) This Agreement specifies the rights and obligations of the parties in connection with the Processor's handling of the controller data in fulfilment of the principal contract.

§ 2 Term and termination of the Agreement

The contract of use between the Parties as well as this Agreement are concluded for an indefinite period of time and may be terminated by either party at any time without stating reasons. Termination of the contract automatically leads to the termination of this Agreement. An isolated termination of this Agreement is excluded.

§ 3 Nature and purpose of the processing, type of personal data, categories of data subjects

(1) The Processor processes the controller data exclusively on behalf of and in accordance with documented instructions from the Controller.

(2) The processing of the controller data shall be carried out in accordance with the provisions on the nature and purpose of data processing contained in Appendix 1 to this Agreement. It refers to the type of personal data specified in Appendix 1 and the categories of data subjects listed therein.

(3) The processing of the controller data takes place within the territory of the European Union or in another contracting state of the Agreement on the European Economic Area. Any relocation to a third country may only take place if the special requirements of Article 44 et seq. of the GDPR are met.

§ 4 Rights and obligations as well as authority of the Controller to issue instructions

(1) The processing of controller data by the Processor within the scope of this Agreement shall be carried out exclusively in accordance with the instructions of the Controller pursuant to Article 28 para. 3 sentence 2 lit. a GDPR, unless the Processor is obliged

to carry out further processing in accordance with the law of the European Union or the law of the Member State to which it is subject. In such a case, the Processor shall notify the Controller of these legal requirements, unless the relevant law prohibits such notification because of an important public interest.

(2) The Controller reserves the right to give comprehensive instructions on the type and purpose of data processing within the framework of the order description agreed in this Agreement, which he can specify in detail by means of individual instructions.

(3) Individual instructions after conclusion of the Agreement require text form and must be documented by both the controller and the processor.

(4) Unless there are obvious indications to the contrary or explicit written information from the controller, the processor may assume that any employee of the controller issuing instructions is authorised to do so.

(5) If the Controller issues individual instructions regarding the processing of controller data that exceed the scope of services agreed in the principal contract, the costs justified thereby shall be borne by the Controller.

(6) The Processor shall not be under any obligation to legally examine the instructions of the Controller. If, however, the Processor is of the opinion that an instruction of the Controller violates data protection provisions, he shall inform the Controller accordingly. The Processor shall be entitled to suspend the execution of the relevant instruction until the instruction has been confirmed or amended. If the Controller does not dispel the doubts of the Processor upon being informed of an instruction which, in the opinion of the Processor, is unlawful, the Processor may refuse to implement the instruction in question insofar as it concerns his sphere of responsibility.

(7) The Controller shall inform the Processor immediately and completely if he discovers errors or irregularities in connection with the processing of controller data by the Processor or his instructions.

§ 5 The Processor's rights and obligations

(1) The Processor shall ensure that the processing within the framework of the performance of the principal contract in his sphere of responsibility, which includes the subcontractors pursuant to § 9 of this Agreement, is carried out in accordance with the provisions of this Agreement.

(2) The Processor shall be obliged to provide the Controller, upon request, with the necessary information, including certifications as well as inspection- and assessment results, which serve as proof of compliance with the obligations laid down in this Agreement.

(3) The Contractor shall obligate in writing the persons authorized to process controller data pursuant to Article 28 para. 3 lit. b GDPR to maintain confidentiality unless they are already subject to an appropriate legal obligation of confidentiality.

(4) The Processor is obliged to designate an expert and reliable data protection officer who can perform his duties in accordance with Article 37, 38 and 39 GDPR as well as § 38 Federal Data Protection Act (BDSG) if and as long as the legal requirements for an order obligation are met. The Processor shall store the current contact details of the data protection officer on his website in an easily accessible form (Article 37 para. 7 GDPR).

(5) The Processor and, if applicable, his representative shall keep a record of processing activities carried out on behalf of the Controller which contains all information pursuant to Article 30 para. 2 GDPR. This obligation does not apply if the requirements of Article 30 para. 5 GDPR are fulfilled.

(6) The Processor is obliged to support the Controller, within the reasonable and necessary limits and against reimbursement of the expenses and costs incurred as a result, in fulfilling his obligations under Article 12 to 22 and Article32 to 36 GDPR. Support shall be provided taking into account the type of processing and the information available to the Processor as well as, where possible, appropriate technical and organisational measures, in particular in response to requests to exercise the rights of the data subject specified in Articles 12 to 22 GDPR.

§ 6 Technical and organisational measures

(1) The Processor shall implement all necessary technical and organizational measures to adequately protect the data of the Controller pursuant to Article 32 GDPR, in particular measures listed in Appendix 2.

(2) As the technical and organisational measures are subject to technical progress and technological development, the Processor shall be permitted to implement alternative and adequate measures, provided that they do not fall below the security level of the measures specified in Appendix 2. The Processor shall document such changes. Material changes to the measures shall require the prior consent of the Controller.

§ 7 The Processor's reporting duties and conduct in the case of infringements

(3) The Processor shall inform the Controller without delay if he determines that he or an employee has violated data protection regulations or provisions of this Agreement when processing controller data, insofar as there is a risk of a violation of the protection of personal data of the Controller within the meaning of Article 4 No. 12 GDPR.

(4) Insofar as the Controller is subject to statutory notification obligations due to an incident pursuant to paragraph (1), the Processor shall support the Controller in fulfilling his/her obligations at the latter's request within the scope of what is reasonable and necessary against reimbursement of the expenses and costs incurred as a result thereof.

(5) The Processor shall immediately take the necessary measures to secure the data and to reduce possible adverse consequences for the data subjects, inform the Controller thereof and request further instructions.

(6) Notifications and information pursuant to Article 33 or 34 GDPR for the Controller may only be made by the Processor following prior instructions from the Controller.

§ 8 The Controller's control and inspection rights

(1) The Controller shall, at his/her own expense, convince himself of the technical and organisational measures taken by the Processor in accordance with Appendix 2 prior and after the commencement of data processing and shall document the results. The control shall be carried out by obtaining a self-assessment from the Processor, which the Processor may also fulfil by submitting a suitable certificate from an expert.

(2) The Processor undertakes to provide the Controller, upon written request, with all necessary information regarding his/her obligations under this Agreement and, in particular, to prove the implementation of the technical and organisational measures of Appendix 2. Proof of such measures, that do not only concern the specific assignment, can be provided by compliance with approved codes of conduct in accordance with Article 40 or certifications in accordance with Article42 GDPR; current certificates, reports or report extracts from independent instances (e.g. auditors, revision, data protection officer, IT security department, data protection auditors, quality auditors); suitable certification by an IT security or data protection audit.

§ 9 Subprocessor relationships

(1) The Processor is entitled to assign further Subprocessors under the condition of a contractual agreement in accordance with Article 28 para. 1 to 4 GDPR. Subprocessors within the meaning of this provision are those service providers who have been directly engaged to render the principal contractual performance. The principal contractual performance does not include ancillary contractual services which the Processor may use such as telecommunication services, mail or haulage services or for the disposal of data carriers or for other measures to ensure the confidentiality, availability, integrity and resilience of hardware and software systems used for data processing. The Processor is however obligated to put appropriate and law-compliant contractual agreements in place and to take appropriate control measures, ensuring data protection and data security for the controller data also with regard to contracted-out ancillary services.

(2) The Controller expressly consents to the assignment of the Subprocessors listed in Appendix 3.

(3) The Processor shall immediately inform the Controller of any intended change with regard to the involvement or replacement of other Subprocessors. The Controller may object to such changes for important reasons to be proven to the Processor. The objection must be made in writing within a period of one week from the date of receipt of a corresponding notification from the Processor.

(4) When a Subprocessor is engaged, the Processor shall impose on that Subprocessor, by way of a contractual agreement or other legal instrument in accordance with European Union law or the law of the Member State concerned, the same data protection obligations as those laid down in this agreement. The contractual agreement must be drafted in such a way that, should the need arise, the Controller can – if necessary – carry out appropriate audits and inspection measures at the Subprocessor's premises, also on-site or to have them carried out by third parties acting on his/her behalf.

(5) If a Subprocessor fails to fulfil the obligations laid down in this Agreement or if such Subprocessor should be in breach of any regulations pertaining to data protection law, the Processor shall be responsible towards the Controller for the Subprocessor's compliance with his/her obligations.

(6) Where Subprocessors in a third country are to be assigned, the Processor shall ensure that the Subprocessor offers guarantees for an adequate level of data protection (e.g. by concluding an agreement based on EU standard data protection clauses).

§ 10 Rights of data subjects

(1) The rights of the data subjects affected by the data processing are to be asserted against the Controller.

(2) In so far as a data subject concerned should directly approach the Processor in order to exercise their rights pursuant to Article 12 to 22 GDPR relating to their personal data, the Processor shall refer the data subject to the Controller.

§ 11 Liability

(1) The Controller and the Processor shall be jointly and severally liable for the compensation of damages incurred by a data subject due to an inadmissible or incorrect processing of personal data within the scope of the contractual relationship.

(2) In the internal relationship with the Processor, the Controller alone is responsible for the compensation of damages suffered by a person concerned due to an inadmissible or incorrect processing of controller data within the scope of order processing in accordance with the applicable data protection law. The Controller alone shall be liable, in the internal dealings between the Controller and the Processor, for any loss or damage incurred by a data subject as result of an inadmissible or incorrect processing of Controller data performed as part of the processor Agreement.

(3) The Controller undertakes to indemnify the Processor internally against all claims by third parties unless and until he can prove that the Processor has not fulfilled his/her obligations under the GDPR which apply specifically to the Processor or has acted in disregard of a lawfully issued instruction from the Controller or contrary to a lawfully issued instruction.

(4) Should a data protection authority or a court impose a fine on the Processor for data processing by the Processor based on the Controller's instruction, the Controller shall reimburse the Processor unless and until he can prove that the Contractor has not fulfilled his/her obligations under the GDPR which apply specifically to the Contractor or has acted in disregard of a legally issued instruction from the Controller or against a legally issued instruction. the pertinent amount following a written notification and in full within 30 days of having received such written notice.

(5) The Controller shall reimburse the Processor for any costs, including legal expenses, resulting from the infringement pursuant to clauses 3 and 4 for which the Controller can be held accountable.

(6) Unlimited liability: The Processor shall assume unlimited liability for intent and gross negligence, for breach of a contractually assured guarantee and as stipulated in the Product Liability Act. In cases of minor negligence, the Processor shall assume liability for any damage or injury to life, limb or health. In all other cases the following limited liability shall apply: In cases of minor negligence the Processor shall only be liable for breaches of material duties or obligations of the principal contract, the fulfilment of which is prerequisite for the proper execution of the principal contract and on which the Controller may reasonably rely (cardinal obligation). In cases of minor negligence, liability shall be limited to the amount of loss or damage which can be typically foreseen at the time of concluding the contract and which is typically to be expected in such cases.

§ 12 Returning and deleting transferred Controller data

(1) The Processor shall return or delete all controller data and destroy existing copies at the discretion of the Controller after termination of the Agreement (in particular in the event of termination or other termination of the main contract), unless an obligation to store the data exists under Union law or the law of the Member States.

(2) The Processor shall document the deletion or destruction of data relating to the Controller and furnish proof of such deletion or destruction to the Controller upon request.

(3) Documentations which serve as proof of the proper data processing in accordance with the instructions or legal retention periods shall be retained by the contractor beyond the end of the contract in accordance with the respective retention periods.

§ 13 Sundry

(1) The Controller and the Processor, and where appropriate, their representatives, shall cooperate in the fulfilment of their duties and requirements, if requests are made by the supervisory authority.

(2) In so far as there are no special provisions in this Agreement, the provisions contained in the principal contract shall apply. In the case of discrepancies between this Agreement and the provisions contained in other agreements, in particular the principal contract, the provisions of this Agreement shall take precedence.

(3) Agreements on the technical and organisational measures and the control and assessment documents (also relating to Subprocessors) shall be kept by both parties for the period of their validity and then for another full three calendar years.

(4) The right to plead the right of retention within the meaning of Section 273 BGB (German Civil Code) shall hereby be excluded with regard to the data processed for the Controller and the pertinent data storage media.

	Berlin, 14.05.2021
....	....
(Place, date)	(Place, date)
....	....
(Controller's signature)	(Processor's signatures)

Appendices:

Appendix 1	Purposes and nature of data processing, type of data and categories of data subjects
Appendix 2	Technical and organisational measures
Appendix 3	Approved Subprocessors

Appendix 1

Purpose and nature of data processing, type of data and categories of data subjects

The Processor shall render the services agreed in this Appendix to the Controller exclusively in accordance with the Controller's instruction and on the basis of the Agreement reached by the parties on the processing of personal data on the Controller's behalf.

The Processor shall process the following personal data on the Controller's behalf for the following purposes:

Type of data	Nature and purpose of data processing	Categories of data subjects
Audio, *Video,* *Username,* *E-mail,* *Profile picture*	*collection, recording, organisation, structuring, storage, adaptation and making available to other end customer to provide video interface and platform to end customer*	*Clients, end customer*

____
Place, date

Berlin, 20.05.2021
Place, date

____
Controller

____
Processor

Appendix 2

Technical and organisational measures pursuant Article 32 GDPR

Description of the technical and organisational measures put in place by Wonder Technologies GmbH, Tempelhofer Ufer 1A, 10961 Berlin, to implement and comply with the requirements stipulated in Article 32 and Article 25 (2) 3rd sentence GDPR.

1. *Transparency*
   Transparency in the sense of Article 5 (1) (a) of the GDPR is ensured if data are processed in a manner that is comprehensible to the data subject. For this purpose, the controller must take appropriate measures pursuant to Article 12 (1) of the GDPR in order to comply with the information and notification obligations pursuant to Articles 13 and 14 of the GDPR and to be able to provide the relevant information in a precise, transparent, comprehensible and easily accessible form in a clear and simple language.

   - Documentation of the nature, extent, circumstances and purposes of the processing
   - Documentation of data recipients (and time span of transfer)
   - Documentation of binding deletion deadlines
   - Documentation of order and suborder relationships
   - Publication of information obligations vis-à-vis affected parties
   - Provision of the information obligations referred to here at the request of the data subject
   - Publication of information on the processing of personal data as data protection information on the homepage

2. *Purpose limitation*
   Purpose limitation in the sense of Article 5 (1) (b) of the GDPR is ensured if the data are collected for specified, unambiguous and legitimate purposes and are not further processed in a manner incompatible with these purposes.

   - Presentation of purposes in the list of processing activities
   - Obligation of employees to comply with the requirements of the GDPR

3. *Data minimization*
   Data minimization within the meaning of Article 5 (1) (c) of the GDPR is ensured if the data is adequate and relevant to the purpose and limited to what is necessary for the purposes of the processing.

   - Data protection by design (data protection by design)
   - Implementation of data protection by default (data protection by default)

- Definition of binding deletion periods
- Regular manual triggering of the deletion of data that is not required
- Anonymization of data when identification is no longer necessary
- Regular audits of the data volume (by the data protection officer)

4. *Accuracy*
   Accuracy within the meaning of Art. 5(1)(d) DSGVO is ensured if the data processed are factually correct and, if necessary, up to date, and data that are inaccurate with regard to the purposes of their processing are deleted or corrected without delay.

   - Proof of the origin of data
   - Immediate deletion of incorrect data
   - Immediate correction of inaccurate data
   - *Request for rectification by electronic submission of a request*
   - *Establishment of a procedure for the rectification of data upon request*

5. *Storage limitation*
   Storage limitation within the meaning of Article 5 (1) (e) of the GDPR is ensured if the data processed are stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.

   - Early anonymization of personal data
   - Early pseudonymization of personal data

6. *Confidentiality*
   Confidentiality in the sense of Article 32 (1) (b) in conjunction with Recital 39 and 83 of the GDPR is sufficiently ensured if unauthorized persons have no access to the data and cannot use the data or the devices with which they are processed and the data are also protected against unauthorized or unlawful processing and against accidental loss in accordance with Article 5 (1) (f) of the GDPR.

   - Security locks
   - Key regulation (determination of authorised personnel)
   - Manual locking system
   - Cleaning personnel committed to data protection
   - User account for each employee
   - Password policies appropriate to the purpose
   - Authentication with password
   - Regulations when employees leave the company
   - Allocation of administrator rights to a minimum number of person*s*
   - disk encryption
   - Destruction of data media in accordance with DIN 66399
   - Separation of productive and test system
   - Consistent transport encryption during e-mail transmission
   - Data communication via VPN tunnel

7. *Integrity*

Integrity within in the sense of Article 32 (1) (b) in conjunction with Article 5 (1) (f) of the GDPR is ensured when data is protected against accidental loss, accidental destruction or accidental damage, i.e. the data is complete, unchanged and intact.

- Encryption of the Internet presence
- Packet Filter Firewall
- Automated update processes for operating systems, applications and services
- Content-encrypted data transmission

8. *Availability*

Availability in the sense of Article 32 (1) (b) of the GDPR is ensured if the data can be used at any time for its intended purpose. In addition, according to Article 32 (1) (c) of the GDPR, the ability to quickly restore the availability of and access to the data in the event of a physical or technical incident must exist.

- Backup and recovery concept (Backup & Recovery)
- Automated creation of data backups (backup)
- Emergency plan for restarting servers and services
- Avoidance of local data storage
- Compromise contingency plan
- Emergency plan in case of data loss
- Automatic notification system in case of failure

9. *Resilience*

According to Article 32 (1) (b), resilience must be ensured on a permanent basis and relates to systems and services in connection with the processing of personal data.

- Automatic notification system when max. load is reached

10. *Accountability and proof of effectiveness*

Accountability according to Art. 5(2) GDPR is fulfilled if the controller can demonstrate compliance with the principles for the processing of personal data. Irrespective of this, pursuant to Art. 32 (1) (d) GDPR, he must be able to regularly review, assess and evaluate the effectiveness of the technical and organizational measures to ensure the security of the processing. In addition, pursuant to Recital 87 of the GDPR, he or she must be able to determine immediately whether a personal data breach has occurred in order to be able to inform the supervisory authority and the data subject without delay.

- Maintenance of a directory of processing activities
- Appointment of a data protection officer
- Documentation of existing IT infrastructure
- Documentation on programs and applications used

- Documentation of the destruction or return of data carriers and documents after completion of an order
- Logging of failed access attempts
- Securing the log data against change and loss
- User ID-related logging
- Random checks on the effectiveness of certain measures

14.05.2021

Date

Signature

Explanatory notes

On 25 May 2018 the GDPR has come into effect immediately in all EU Member States. The requirements it stipulates include that the Controller responsible for the processing of personal data shall take appropriate technical and organisational measures to assure an appropriate standard of protection for data processing. These measures are not prescribed in detail. The Controller is free in determining such measures. The authorative requirement placed on the respective precautionary measures is set forth in Article 32 (1) half-sentence. 2 GDPR, so that

> *"taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk"*

is ensured.

Compliance with the technical and organisational measures pursuant to Article 25, 32 GDPR is one of the data protection regulations which in case of breaches are punishable with a fine of up to 10 million euros or 2% of total world-wide annual sales in the previous business year pursuant to the catalogue of fines in Article 83 (4)a) GDPR. Strict and well-documented compliance with this article can be of great advantage if a data breach occurs.

A. Minimum measures

These are the minimum measures that must be taken:

1. Encryption

Every processing activity is to be assessed as to whether its purpose can also be realised without direct personal reference. If this is the case, readable information is to be converted by an appropriate method into a string which is not easily interpretable.

2. Pseudonymisation

Every processing operation is to be assessed as to whether its purpose can also be realised without direct personal reference. If this is the case, the processing of personal data is to be performed in a manner such that these data can no longer be associated to a specific data subject without reference to additional information. This additional information is to be stored separately and is itself subject to technical and organisational measures intended to ensure that the personal data cannot be associated to an identified or identifiable natural person.

3. Confidentiality

This means that the data are not accessible for unauthorised third parties.

4. Integrity

Is to be understood to mean that the data cannot be falsified.

5. Availability

Refers to the availability of systems for use at all times.

6. Resilience

Means that systems and services must be able to withstand a certain measure of use.

7. Availability assurance

Means the assurance of the capacity to rapidly restore the availability of personal data and access thereto after a physical or technical incident.

8. Measures to verify, assess and evaluate the effectiveness of technical and organisational measures

Companies need to establish a procedure which allows them to regularly assess and evaluate the effectiveness of measures.

B. State of the art

This requires that the state of the art be taken into account. It does not however refer to methods which have just recently been newly developed, but to such measures which have already been proven to be appropriate and effective in practical use and which assure a sufficient level of security. The term "state of the art" implies that a present-day assessment is involved and that the state of the art must be regularly checked as to whether it is up-to-date to be able to guarantee data security. Based on the IT Security Act, the Bundesverband IT-Sicherheit e.V. (Federal Association for IT Security) (TeleTrusT) has published a handout intended to serve as a guideline for those responsible for determining the state of the art in IT security:

https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

In addition, it is always to be borne in mind what the German Federal Office for Information Security (BSI), the supervisory authorities and professional associations refer to as "state of the art", hence it is a continuous updating process.

C. Appropriate level of protection

Article 32 (2) GDPR stipulates an "appropriate level of security" for all data security measures. Thus, data security does not need to be "optimal" or the "best possible" but should be closely geared to the risks which are associated with the respective processing operations. The level of protection is geared to the need for protection of the individual stored personal data records. Hence, the needs for protection should be established by identifying the respective required level of protection for the different types of personal data. This involves that the typical loss or damage scenarios are first identified in order to subsequently deduce the need for protection for the individual types of personal data. A proven approach so far has been classification into protection categories, whereby it might be helpful, for example, to use the categories of the BSI standard 100-2 "normal", "high" and "very high" as guidance. The term "appropriate" takes into account the state of the art, implementation costs, nature and scope of circumstances, purpose of the processing and the various probabilities of occurrence and severity of the risk for the rights and freedoms of natural persons. This procedure should be repeated at regular intervals.

Appendix 3

Approved Subprocessors

Company Subprocessor	Address/ Country	Services provided
Twilio	San Francisco, Kalifornien, USA	Twilio and Sendgrid are services by Twilio Inc. that we use to facilitate audio and video connections between the end customer and his chat partners on a global low-latency network.
Digital Ocean	New York City, New York, USA	Digitalocean is a service by DigitalOcean, LLC and a service platform for database storage.
Amazon Web Services (AWS)	Seattle, Washington, USA	Amazon Web Services is a service by Amazon Inc. and a service platform for database storage.
Agora	Baltimore, Maryland, USA	Agora is a service by Agora Inc. that we also use to facilitate audio and video connections between the end customer and his chat partners on a global low-latency network.
Intercom	San Francisco, Kalifornien, USA	Intercom is a service by Intercom, Inc. and used as a help and support software.
Mailchimp	Atlanta, Georgia, USA	Mailchimp is a service for email marketing automation.

____
Place, date

Berlin, 14.05.2021
Place, date

____
Controller

____
Processor