

Data Processing Agreement (DPA)

between

...

- Data Controller –

hereinafter also referred to as “Client”

and the

MessengerPeople GmbH

Herzog-Heinrich-Str. 9

DE-80336 München

- Data Processor –

hereinafter referred to as “Contractor”

1. Definitions

(1) In accordance with Art. 4 para. 7 GDPR, the Client shall determine the purposes and means of processing of personal data.

(2) In accordance with Art. 4 para. 8 GDPR, the Contractor shall process personal data on behalf of the Client.

(3) According to Art. 4 para. 1 GDPR, Personal Data are all information relating to an identified or identifiable natural person (hereinafter "data subject"); an identifiable natural person is defined as an individual who can be identified directly or indirectly, in particular by assignment to an identifier such as a name, an identification number, location data, an online identifier or to one or more special features that express the physical, physiological, genetic, psychological, economic, cultural or social identity of this natural person.

(4) According to Art. 4 para. 2 GDPR, Processing means any transaction or series of transactions carried out with or without the aid of automated procedures in connection with personal data such as the collection, acquisition, organisation, sorting, storage, adaptation or modification, reading, querying, use, disclosure by transmission, dissemination or any other form of provision, comparison or linking, restriction, deletion or destruction.

2. Subject matter and duration of the agreement

(1) Subject matter

The Contractor shall provide services to the client in the area of communication via existing messengers of various third-party providers (hereinafter also referred to as “Messenger Services”) on

the basis of the Contractor's General Terms and Conditions applicable at the time the order is placed (hereinafter referred to as the Order).

(2) Duration

The duration of this agreement corresponds to the term of the order, provided that the following provisions do not result in additional obligations or rights of termination.

(3) In order to specify the rights and obligations under the applicable data protection regulations for both parties, the parties enter into the present agreement. In case of doubt, the provisions of this agreement take precedence over the provisions of the order.

(4) The provisions of this agreement shall apply to all activities connected with the order in which the contractor and his employees or agents come into contact with personal data originating from or collected for the client.

3. Specifications of Processing

(1) The data processing, in particular the storage and use of customer and end user data for the purpose of providing the Messenger Services, shall take place exclusively in a Member State of the European Union or in another state party to the Agreement on the European Economic Area. Any transfer to a third country requires the prior consent of the Client and may only take place if the special requirements of Art. 44 ff. GDPR are fulfilled.

(2) The limitation of para.1 shall not apply if the Contractor transmits data and information to the client as intended via a third-party messenger to its customer/end user/subscriber with the Client's consent being deemed granted.

(3) The limitation of para. 1 shall equally not apply if the Contractor transmits data and information to his employees via e-mail at the request of the Client in accordance with the contractual provisions with the Client's consent being deemed granted.

4. Right of Instruction

(1) The Contractor may only collect, process or use data within the scope of the order and in accordance with the Client's instructions, in particular, with regard to the transfer of personal data to a third country or an international organisation. Where the law of the European Union or of the Member State, to which the Contractor is subject, requires the Contractor to carry out further processing, the Contractor shall inform the Client thereof before the beginning of the Processing.

(2) The Processing instructions shall be initially provided by the Client and can then be changed, supplemented or replaced in writing. The Client shall issue appropriate individual instructions at any time, specifically regarding the correction, deletion and blocking of data.

(3) All instructions given shall be documented by both the Client and the Contractor. Instructions that supersede the agreed performance level shall be treated as a request for a change in performance.

(4) If the Contractor is of the opinion that an instruction provided by the Client violates applicable data protection regulations, the Contractor shall inform the Client thereof immediately. The Contractor is entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the Client. The Contractor may refuse to carry out an obviously unlawful instruction.

5. Type of Data processed and Data Subjects

(1) Type and purpose of the intended processing of data

Detailed description of the subject matter of the order with regard to the type and purpose of the Contractor services: Storage and use of Client and end user data for the purpose of providing the services.

(2) Categories of data subjects

The categories of data subjects concerned by the processing include:

- Customers/End User/Subscribers of the Client

The Client communicates with these persons via the messenger service and uses certain personal data for this purpose.

- employees of the Client

The processing of personal data for this type of persons shall be deemed agreed between the parties, certain personal data are administered.

(3) Type of data

The subject of the processing of personal data are the following data types/categories (enumeration/description of data categories)

Customers/End User/Subscriber/Employees of the Client

- Last name, first name, profile picture and other profile data, if applicable
- communication data (e.g. telephone numbers, e-mail addresses)
- chat history and derived data.

6. Technical and Organizational Measures

(1) The Contractor shall document the implementation of the requisite technical and organizational measures in advance of the execution of the order and before the start of processing, in particular, with regard to the concrete execution of the order and provide the lists to the Client for inspection purposes. If accepted by the Client, the documented measures shall become the basis of the order. If the Client inspection/audit reveals a need for adjustment, such shall be implemented by mutual agreement.

(2) The Contractor shall guarantee the security level pursuant to Art. 28 para. 3 lit. c, 32 GDPR, in particular in connection with Art. 5 para. 1, para. 2 GDPR. Overall, the measures to be taken shall ensure a level of protection of data security appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. The state-of-the-art level of security, the implementation costs and the type, scope and purpose of processing as well as the different probability of occurrence and severity of the risk to the rights and freedoms of data subjects within the meaning of Art. 32 para. 1 GDPR shall be taken into account in accordance with Annex 1.

(3) The technical and organisational measures are subject to technical progress and further development. Hereby, the Contractor is authorized to implement alternative adequate measures. The safety level of the defined measures may not fall below the agreed standards. Contractor shall document significant changes and provide to the Client for inspection and acceptance.

7. Correction, Restriction and Deletion of Data

(1) The Contractor may not correct, delete or restrict the processing of the data upon its own decision but only upon the documented instructions of the Client. If a data subject contacts the Contractor directly in regard hereto, the Contractor shall immediately forward such request to the Client.

(2) Insofar as the scope of services includes the deletion concept, the right to be forgotten, the obligation of correction and the data portability, such shall be ensured directly by the Contractor in accordance with the documented instructions of the Client.

When an end customer/end user/subscriber to the Client's chat requests the deletion of all of his/her data (to be accomplished by the Client), the following course of actions shall take place:

- a) deletion of all chats and all derived profile data are deleted from the database;
- b) deletion of the user entry incl. phone number after 1-2 hours; the delay is necessary in order for the customer/end user/subscriber to be deleted from the app's broadcast list and for the statistics to be updated;
- c) after the deletion from the databank, information about the customer/end user/subscriber is still available in the back up data, which is deleted after 61 days at the latest, see also point 13 (4).

8. Quality Assurance and other Obligations of the Contractor

In addition to complying with the regulations of this order, the Contractor shall fulfill its legal obligations pursuant to Articles 28 to 33 GDPR; in respect hereto, the Contractor shall guarantee compliance with the following requirements:

- a) written appointment of a data protection officer who shall perform his duties in accordance with Articles 38 and 39 GDPR;
- b) the Contractor's current contact details shall be easily accessible on the homepage;
- c) maintaining confidentiality in accordance with Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. In carrying out the processing order, the Contractor shall only use employees who are bound to confidentiality and who have been appropriately informed beforehand about the relevant data protection provisions. The Contractor and any employee and sub-contractor used who have access to personal data may process such data exclusively in accordance with the instructions of the Client including the powers granted in this order, unless they are legally obliged to process them.
- d) the implementation and compliance with all technical and organisational measures required for this order in accordance with Art. 28 para. 3 sentence 2 lit. c, 32 GDPR in accordance with Annex 1
- e) Upon request, the Client and the Contractor shall cooperate with the supervisory authorities in the performance of their tasks
- f) Immediate information to the Client with regard to control actions and measures taken by the supervisory authority in so far as such may relate to this order. This also applies in cases a competent authority decides to conduct investigations in the context of administrative or criminal proceedings with regard to the processing of personal data on behalf of the Controller.
- g) Insofar as the Client is subject to an inspection by the supervisory authority, administrative or criminal proceedings, the liability claim of a data subject or a third party or any other claim in connection with the processing data on behalf of the controller, the Contractor shall support Client to the best of its ability.
- h) The Contractor shall regularly monitor internal processes and technical and organisational measures to ensure that the processing of data within its area of responsibility is carried out in accordance with the requirements of the applicable data protection legislation and that the rights of the data subjects are protected.

- i) Verifiability of the technical and organisational measures taken vis-à-vis the Client shall remain within the scope of the control powers in accordance with this clause.

9. Subcontracting

(1) Subcontracting within the meaning of this provision shall be understood to define such services that relate directly to the provision of the services in accordance with this Agreement. However, the collection of any data from or transmission of data to a Messenger Service is not to be understood as a subcontracting relationship in as far as another processor in the relationship between the Contractor and the operator of the respective Messenger Service may be concerned. Sub-contractual relationships shall equally not include such ancillary services used by the Contractor with regard to the means of transmission, e.g. telecommunication services and post/transport services. However, in order to guarantee appropriate data protection and data security level of the Client data, the Contractor shall take appropriate and legally required control measures with regard to the outsourced ancillary services as well.

(2) The Contractor may only engage subcontractors (e.g. further data processors) with the prior express written or documented consent of the Client.

- a) The Client agrees to the engagement of the following subcontractor upon a pre-condition of a contractual agreement in accordance with Art. 28 para. 2-4 GDPR:

Subcontractor	Address	Service
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen, Germany	Provision of the data center infrastructure, per which the service is offered.

- b) The outsourcing to subcontractors or the change of the existing sub-contractor is permitted if
- the Contractor notifies the Client of such outsourcing to sub-contractors in writing in advance;
 - the Client does not object to the planned outsourcing in writing until the data is handed over to the sub-contractor; and
 - a contractual agreement in accordance with Art. 28 para. 2-4 GDPR is implemented as a basis of sub-contracting.

(3) The transfer of the personal data to the sub-contractor and its processing are only permitted if all requirements for sub-contracting are met.

(4) If the sub-contractor performs the agreed service outside the EU/EEA, the Contractor shall take appropriate measures to ensure the compliance with the EU data protection regulations. The same applies if service providers within the meaning of para. 1 sentence 2 of this clause shall be used.

(5) Further outsourcing by the sub-contractor requires the express consent of the Client in writing; all provisions in the contract chain shall also be imposed on the following sub-contractors as well.

10. Control Rights of the Client

(1) The Client has the right to carry out appropriate inspections in consultation with the Contractor or to have them carried out by inspectors to be appointed in individual cases in order to ensure the

Contractor's compliance with this agreement by means of checks, of which the Contractor shall be notified in due time and order.

(2) The Contractor shall ensure that the Client may ensure that the obligations of the Contractor pursuant to Art. 28 GDPR have been duly fulfilled. The Contractor undertakes to provide the Client with the necessary information upon request, in particular, with regard to evidence of the implementation of the technical and organisational measures.

(3) Proof of such measures, which do not only concern the specific order, can be provided by means of

- compliance with approved rules of conduct in accordance with Art. 40 GDPR;
- certification according to an approved certification procedure in accordance with Art. 42 GDPR;
- current certificates, reports or report extracts from independent bodies (e.g. auditors, data protection officers, IT security department, data protection auditors, quality auditors);
- a suitable certification by IT security or data protection audit.

(4) If the Client arranges for an audit of the Contractor or its sub-contractors, the Contractor can assert a claim for remuneration customary in the industry, which covers any travel costs, external hosting provider expenses and expenses incurred by the contractor's data protection officer. Such costs shall be agreed between the Client and the Contractor before the start of the inspection.

11. Notification of Breach by the Contractor

(1) The Contractor shall assist the Client in complying with the obligations referred to in Articles 32 to 36 of the GDPR concerning the security of personal data, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations. This includes inter alia the obligations to

- a) ensure an adequate level of protection through technical and organisational measures which take into account the circumstances and purposes of the processing as well as the predicted probability and severity of a possible infringement of rights due to security gaps and enable an immediate determination of relevant infringement events;
- b) report violations of personal data to the Client without undue delay;
- c) support the Client in its duty to inform the data subject and to make all relevant information available without undue delay;
- d) support the Client with regard to its data protection impact assessment, and
- e) assist the Client with regard to consultations with the supervisory authorities.

(2) The Contractor may claim compensation for support services that are not included in the service description or are not attributable to misconduct or violation of contractual provisions on its part.

12. Liability

(1) The parties shall be jointly and severally liable to the data subject concerned for any damage caused by processing that does not comply with the GDPR.

(2) The Contractor is exclusively liable for damages based on a processing, in which the Contractor

- a) has failed to fulfil the obligations arising from the GDPR and specifically imposed on data processors; or
- b) acted in breach of the lawful instructions of the Client.

(3) Further liability claims according to general laws remain unaffected.

13. Completion of the Order

(1) The Contractor shall return to the Client all documents, data and data carriers made available to him or delete them at any time after completion of the order or per request, unless there is an obligation under EU or German law to store the personal data. This also applies to any data backups stored by the Contractor. The Contractor shall also provide documented proof of the proper deletion of any data still available.

(2) The Client has the right to verify the complete and contractual return or deletion of the data that were in the Contractor's possession in an appropriate manner.

(3) The Contractor shall treat all data, which have become known to him in connection with the order, even after the ending of the order, confidentially. The present agreement shall remain valid beyond the ending of the order as long as the Contractor possesses personal data, which has been provided by the Client or collected on the Client's behalf.

(4) The Client's personal data shall be deleted 28 days upon ending of the Agreement. With regard to the backup storage, the data shall be available for a maximum of 61 days.

14. Final Provisions

(1) Amendments and supplements to this Agreement shall be made in writing to be valid. This also applies to the waiver of this formal requirement. The priority of individual contractual agreements remains unaffected.

(2) Should individual provisions of this agreement be or become wholly or partly invalid or unenforceable, this shall not affect the validity of the remaining provisions.

(3) This agreement is subject to German law. Exclusive place of jurisdiction is Munich.

Attachment - Technical and Organisational Measures of MessengerPeople GmbH (Art. 32 GDPR)

Attachment - Technical and Organisational Measures of MessengerPeople GmbH (Art. 32 GDPR)

Scope	Subject matter	Measures
Pseudonymization and encryption (Art. 32 para. 1 lit. a GDPR)		
	Encryption	
		Editors' passwords are stored as a hash with a salt
Confidentiality (Art. 32 para. 1 lit. b GDPR)		
	(Physical) Access control	
		Electronic access control system with logging (Hetzner)
		Documented allocation of keys to employees and colocation clients for colocation racks (each client exclusively for his colocation rack) (Hetzner)
		Guidelines for accompanying and providing identification to visitors in the building (Hetzner)
		24/7 staffing of the data centers (Hetzner)
		Video surveillance (Hetzner)
		Documented allocation of keys to employees
		Special key with copy protection
	(Electronic) Access control	
		Password assignment (lower and upper case letters, special characters, numbers, min. 8 characters, regular changes, password history)
		Regular change of passwords
		Screen lock in absence with password activation
		Role-related rights are linked to access IDs (grouping by administrator, user, etc.)
	Authorization control	
		Demand-oriented design of the authorization concept and access rights as well as their

		monitoring and logging
		Written authorization concept and a programmatic authorization concept
		Clear Desk Policy
		Only a small group of administrators has access to the database
		Controlled destruction of data carriers (paper by shredder)
		Antivirus software including regular security updates and patches
	Separation control	
		The Client data is processed separately and is separated from each other by unique identifiers
		Contract information and subscriber's information are stored in different databases.
Integrity (Art. 32 para. 1 lit. b GDPR)		
	Handover control	
		The data transfer from the Client to the Contractor can be accomplished per different methods and shall be agreed between the parties. Normally, the data is provided via the customer interface. The transmission is encrypted with SSL.
		The Contractor supports common secure variants.
		Encrypted tunneling of connections or secure transmission via VPN
	Data storage medium control	
		Using private data storage medium at workplace is prohibited
	Input control	
		Subscriber status changes are recorded
		People identifiable characteristics (phone number) can not be changed through the customer interface.
		Mutual surveillance (4 eyes principle)
		Logging of changes

Availability and resilience (Art. 32 para. 1 lit. b and c GDPR)		
	Availability check	The database is mirrored online. The mirroring can be activated using failover IPs
		A backup procedure has been set up
		Use of uninterruptible power supply
		Virus protection is installed
Procedure for regular testing, assessing and evaluating (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)		
	Resilience	
		Emergency planning is available and documented in emergency concepts
		The functionality of concepts is tested at regular intervals (usually annually)
		Emergency plans are subject to a regular review and improvement process
	Incident-response-management	
		A ticket system ensures the prompt processing of all inquiries
	Data protection by design and by default (Art. 25 Abs. 2 GDPR)	
		Double-opt-in-procedure
	Processing on behalf of a controller	
		Processing on behalf of Controller within the meaning of Art. 28 GDPR does not take place without corresponding instructions from the Client.
		Regular inspection of subcontractors