Data Processing Agreement (DPA)

between

[FIRMA]
[ADRESSE1]
[ADRESSE2]
[PLZ] [ORT]

- controller - hereinafter referred to as the– client -

and the

MessengerPeople GmbH
Herzog-Heinrich-Str. 9
80336 München

- processor – hereinafter referred to as - contractor -

1. Definitions

(1) Client according to Art. 4 para. 7 GDPR is the body that decides on the purposes and means of processing personal data.

(2) In accordance with Art. 4 para. 8 GDPR, the contractor is the body that processes personal data on behalf of the data 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 one 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 contract

(1) Subject matter

The Contractor provides various 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 order (term) 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 data protection law 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 contract 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. Specification of the content of the order

(1) In principle, the Contractor's 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 does not apply if the contractor transmits data and information for the client as intended via a third-party messenger to its customer/end user/subscriber. The client's consent is deemed to have been given for this.

(3) The limitation of paragraph 1 shall also not apply if the contractor transmits data and information to his employees via a mail provider at the request of the customer in accordance with the provisions. The client's consent shall be deemed to have been granted in this respect.

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 instructions of the client; this applies 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 States to which he is subject requires the contractor to carry out further processing, he shall inform the client of these legal requirements before processing.

(2) The instructions of the client are initially determined by this order and can then be changed, supplemented or replaced by the customer in written form by individual instructions (individual instructions). The client is entitled to issue appropriate individual instructions at any time. This includes instructions regarding the correction, deletion and blocking of data.

(3) All instructions given shall be documented by both the client and the contractor. Instructions that go beyond the agreed performance are treated as a request for a change in performance.

(4) If the contractor is of the opinion that an instruction of the customer violates data protection regulations, he must inform the client 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, circle of 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's tasks: Storage and use of customer and end user data for the purpose of providing the Messenger 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

These persons act in the relationship between the client and the contractor, whereby 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 Principal

- 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 organisational measures

(1) The contractor shall document the implementation of the technical and organisational measures set out and required in advance of the award of the order before the start of processing, in particular with regard to the concrete execution of the order, and hand them over to the customer for inspection. If accepted by the client, the documented measures become the basis of the order. If the client inspection/audit reveals a need for adjustment, this must be implemented by mutual agreement.

(2) The contractor shall provide the security 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 are measures of data security and to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. The state of the art, 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 must be taken into account[details in Annex 1].

(3) The technical and organisational measures are subject to technical progress and further development. In this respect, the contractor is permitted to implement alternative adequate measures. The safety level of the defined measures must not be undershot. Significant changes must be documented.

7. Correction, restriction and deletion of data

(1) The contractor may not correct, delete or restrict the processing of the data which are processed in the order on his own authority but only after the documented instructions of the client. If a data subject contacts the contractor directly in this regard, the contractor shall immediately forward this request to the client.

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

When the client deletes a customer/end user/subscriber manually over the user interface, the following actions will occur:

a) All chats and all derived profile data will immediately be deleted from the database.
b) The user entry with the phone number will be deleted after 1-2 hours. The delay is necessary in order for the customer/end user/subscriber to be taken out of the App's broadcast list and for the statistics to be updated.
c) After the deletion from the data bank, information about the customer/end user/subscriber is still available in the back up data. This will be rewritten after 61 days at the latest.

8. Quality assurance and other obligations of the contractor

In addition to complying with the regulations of this order, the contractor has legal obligations pursuant to Articles 28 to 33 GDPR; in this respect, in particular, he guarantees compliance with the following requirements:

a) Written appointment of a data protection officer who performs his duties in accordance with Articles 38 and 39 GDPR.
b) The contractor's current contact details are easily accessible on the contractor's homepage.
c) Maintaining confidentiality in accordance with Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. In carrying out the work, the contractor shall only employ employees who are bound to confidentiality and who have been informed beforehand about the data protection provisions relevant to them. The contractor and any person subject to the contractor who has 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[details in Annex 1].
e) On request, the client and the contractor shall cooperate with the supervisory authority in the performance of their tasks.
f) Immediate information to the client on control actions and measures taken by the supervisory authority in so far as they relate to this order. This also applies if a competent authority investigates in the context of administrative or criminal proceedings with regard to the processing of personal data during processing data on behalf of the controller at the contractor.
g) Insofar as the client for his part 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 with the contractor, the contractor must support him to the best of his ability.
h) The contractor shall regularly monitor internal processes and technical and organisational measures to ensure that processing within his area of responsibility is carried out in accordance with the requirements of the applicable data protection legislation and that the rights of the data subject are protected.
i) Verifiability of the technical and organisational measures taken vis-à-vis the client within the scope of his control powers in accordance with Clause 8 of this contract.

9. Subcontracting relationships/ another processor

(1) Subcontracting relationships within the meaning of this provision shall be understood to mean those services which relate directly to the provision of the principal service. The collection of any data from or transmission of data to a Messenger is not to be understood as a subcontracting relationship in the means of engaging another processor in the relationship between the contractor and the operator of the respective Messenger. Sub-contractual relationships are also not such ancillary services which the contractor uses e.g. as telecommunication services and post/transport services.

However, in order to guarantee data protection and data security of the client's data, the contractor is obliged to take appropriate and legally compliant contractual agreements and control measures, even in the case of outsourced ancillary services.

(2) The contractor may only commission subcontractors (another processor) with the prior express written or documented consent of the client.

a) The client agrees to the assignment of the following subcontractors on condition of a contractual agreement in accordance with Art. 28 para. 2-4 GDPR:

Subcontractor	Address	Service
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen	Provision of the infrastructure through which the service is offered.
Google Ireland Ltd.	Gordon House, Barrow Street Dublin 4 Ireland	Provision of the infrastructure through which the service is offered.
Stripe Payments Europe Ltd.	C/O A&L Goodbody Ifsc North Wall Quay Dublin 1 Ireland	Processing Payment, storing and processing customer data and subscriptions, invoicing.
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy L-1855 Luxembourg	File/Media permanent storage.

b) The outsourcing to subcontractors or the change of the existing subcontractor is permitted, insofar as:

- the contractor notifies the client of such outsourcing to subcontractors in writing or in text form in advance and

- the client does not object to the planned outsourcing to the contractor in writing or in text form until the time of handover of the data and

- a contractual agreement in accordance with Art. 28 para. 2-4 GDPR is taken as a basis.

(3) The transfer of the client's personal data to the subcontractor and his first action are only permitted if all requirements for subcontracting are met.

(4) If the subcontractor performs the agreed service outside the EU/EEA, the contractor shall take appropriate measures to ensure the admissibility under data protection law. The same applies if service providers within the meaning of para. 1 sentence 2 are to be used.

(5) Further outsourcing by the subcontractor requires the express consent of the contractor (at least in text form); all contractual provisions in the contract chain must also be imposed on the other subcontractor.

10. Control rights of the client

(1) The client has the right to carry out inspections in consultation with the contractor or to have them carried out by inspectors to be appointed in individual cases. He has the right to satisfy himself of the contractor's compliance with this agreement in his business operations by means of spot checks, which as a rule must be notified in good time.

(2) The contractor shall ensure that the client can satisfy himself that the obligations of the contractor pursuant to Art. 28 GDPR have been fulfilled. The contractor undertakes to provide the client with the necessary information on request and in particular to provide 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

- 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, auditors, data protection officers, IT security department, data protection auditors, quality auditors);
- a suitable certification by IT security or data protection audit (e.g. according to BSI-Grundschutz)

(4) If the client arranges an audit of the contractor or his subcontractors, 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. These costs shall be agreed between the client and the contractor before the start of the inspection.

11. Notification of breaches 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, among other things

a) ensuring 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) the obligation to report violations of personal data to the client without undue delay
c) the obligation to support the client in its duty to inform the data subject and to make all relevant information available to him without undue delay in this connection
d) the support of the client for its data protection impact assessment
e) assisting the client in prior consultations with the supervisory authority

(2) The contractor can claim compensation for support services that are not included in the service description or are not attributable to misconduct on the part of the contractor.

12. Liability

(1) The client and the contractor 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 which are based on a processing carried out by him, in which

a) he has failed to fulfil the obligations arising from the GDPR and specifically imposed on processors; or
b) he acted in breach of the lawful instructions of the client; or
c) he has acted against the lawfully given instructions of the client.

(3) Insofar as the client is obliged to pay damages to the data subject, he shall reserve the right of recourse to the contractor.

(4) In the internal relationship between client and contractor, however, the contractor shall only be liable for damage caused by processing if he

a) has failed to fulfil its specific obligations under the GDPR; or
b) has acted in breach of or against the lawful instructions given by the client.

(5) 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 - at the request of the client, unless there is an obligation under Union law or the law of the Federal Republic of Germany to store the personal data - delete them at any time after completion of the order or at his request. This also applies to any data backups at the contractor. The contractor shall provide documented proof of the proper deletion of any data still available.

(2) The client has the right to check the complete and contractual return or deletion of the data at the contractor in an appropriate manner.

(3) The contractor is obligated to treat confidentially the data which have become known to him in connection with the order even after the end of the order. The present agreement shall remain valid beyond the end of the order as long as the contractor has personal data which has been provided to him by the client or which he has collected for him.

(4) The client's personal data will be deleted 28 days after ending the contract. In the backup, the data will be available for a maximum of 61 days.

14. Final provisions

(1) Amendments and supplements to this agreement must be made in written form. This also applies to the waiver of this formal requirement. The priority of individual contractual agreements remains unaffected by this.
(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.

Attachments:

Technical and organisational measures (Art. 32 GDPR)

Attachment - technical and organisational measures (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 marking guests in the building (Hetzner)
		24/7 staffing of the data centers (Hetzner)
		Video surveillance at the inputs and outputs (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 subscribers 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 take place in different ways and must be agreed between the partners. 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 mirror can be activated using failover IPs
		A backup procedure has been set up
		Use of uninterruptible power supply
		Virus protection are 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 these 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 a controller within the meaning of Art. 28 GDPR does not take place without corresponding instructions from the client/controller.
		Regular inspection of subcontractors