Data processing agreement

according
to the EU General Data Protection Regulation
(GDPR)

between the

Customer

- hereinafter referred to as the “Controller” -

and **Zeeg GmbH**

- hereinafter referred to as “Processor” -

- both hereinafter jointly referred to as “Contracting Parties”

the following agreement on order processing is concluded:

Contracting parties

Customer

Company:	_____
Address:	_____
Country:	_____
Registration number:	_____
Represented by:	_____

Processor

Company:	Zeeg GmbH
Address:	Friedrichstraße 114a, 10117 Berlin
Country:	Germany
Registration number:	HRB 253807
Represented by:	Florian Horbach, Mohammad Moghaddas

Content

§ 1 Scope of application and definitions 4
§ 2 Specification of the contract's contents 4
§ 3 Responsibility and authority to issue instructions 6
§ 4 Compliance with mandatory legal obligations by the processor 7
§ 5 Technical and organizational measures and their control 8
§ 6 Notification of breaches by the processor 8
§ 7 Deletion and return of data 9
§ 8 Subcontractors 9
§ 9 Data protection control 10
§ 10 Other provisions 11
§ 11 Final provisions 11
Annex 1 "Technical and Organizational Measures" 12
§ 1 Technical and organizational security measures 12
§ 2 Internal organization of the processor 12
§ 3 Specification of the individual measures 12
Annex 2 "Subprocessors" 15
Annex 3 "Contact and communication" 16

§ 1 Scope of application and definitions

The agreement applies to the processing of all personal data that is the subject of the service agreement or arises in the course of its implementation or becomes known to the processor. All terms in this agreement that have an equivalent in the GDPR are based on the respective legal understanding of the GDPR.

§ 2 Specification of the contract's contents

(1) The object of the commissioned processing as well as the scope, type and purpose of the intended processing of personal data are determined by the service agreement and this agreement on commissioned processing. The general terms of use (https://zeeg.me/en/legal/terms) constitute the service agreement and are expressly agreed to by the controller upon registration.
(2) The term of this agreement corresponds to the term of the service agreement. If the Service Agreement can be terminated by ordinary notice, the provisions of the Service Agreement shall apply. In case of doubt, termination of the Service Agreement shall also be deemed termination of this Agreement and termination of this Agreement shall be deemed termination of the Service Agreement. The controller is entitled to terminate this agreement at any time for good cause. This must be done in accordance with Annex 3 "Contact and communication". Good cause shall be deemed to exist in particular if the processor intentionally or grossly negligently violates provisions of the GDPR or is unable or unwilling to carry out an instruction of the controller. In particular, such good cause exists in the cases of Section 8 (1) and Section 11 (1) of this agreement. In the case of simple - i.e. neither intentional nor grossly negligent - violations, the controller shall first set the processor a reasonable deadline within which the processor can remedy the violation. If this period expires without result, the controller then has the right to extraordinary termination.
(3) The following types or categories of data are subject to processing by the processor:
Types of data

i. Controller and persons authorized by the Controller to use the account (collectively "Users"): Identification and contact data (name, contact data, user name, company/organization data); employment/organization data (geographical location, website), contact information (email address, IP address, date and time), content uploaded by the user as well as content created in the platform

ii. Contact persons of the controller: Identification and contact data as uploaded by the user (name, e-mail address); IT information (IP addresses, opening/click rate, online navigation data), information shared by contact person.

(4) The following categories of persons are affected by the handling of the corresponding personal data:

Categories of persons

i. Users and

ii. any person

- whose e-mail address or telephone number is included in the customer distribution list,
- whose information is stored or collected via the functionalities of the Platform (“Processor Services”),
- to whom Users send emails or with whom they otherwise contact or communicate via the Processor Services (collectively, “Subscribers”).

(5) Scope, type and purpose of data processing: Electronic processing of personal data in accordance with section 3 takes place using the services of the processor by the controller. The use of the processor's services is based on the use by the controller and this data processing agreement and represents the controller's final instructions to the processor. The use of the services of the processor by the controller leads - depending on the use - to operations or series of operations carried out with or without the aid of automated procedures in connection with personal data in accordance with paragraph 3, which may include in particular the collection, recording, organization, sorting, storage, retrieval, consultation, use, disclosure by transmission or any other form of provision, comparison or linking, restriction, erasure or destruction.

The data processing follows the purpose underlying the respective service use by the controller, in particular for the management of business relationships with contact and recipient persons, for communication with contact and recipient persons, for direct marketing and for transaction communication with contact and recipient persons. The processor can check availability in linked calendars, create, edit and delete appointments, insofar as this is technically possible for the controller.

In order to provide a secure and efficient service, the Processor processes the Personal Data to detect, monitor and prevent fraud, phishing, unsolicited communication or any other unauthorized behavior towards the Processor's platform, infrastructure or service in accordance with applicable data protection laws and regulations and in accordance with the Processor's

privacy policy (https://zeeg.me/en/legal/privacy). This processing is necessary for the provision of the Processor's standard SaaS service.

§ 3 Responsibility and authority to issue instructions

(1) The Controller may export, correct, adjust and delete the processing of the personal data in its account at any time.
(2) In order to ensure the protection of the rights of the data subjects, the processor shall support the controller if the controller is not able to ensure this protection alone. In particular, the processor shall provide support by ensuring appropriate technical and organizational measures within the meaning of Art. 32 GDPR.
(3) If a data subject contacts the data processor directly to assert a data subject right, the data processor shall immediately refer the data subject to the data controller if the data controller is identified in the data subject's request. The processor shall assist the data subject in identifying the controller if the data subject provides sufficient information in this regard. The processor shall not be liable if the controller fails to respond to a data subject's request within the scope of the rights under section III, or fails to respond correctly or on time.
(4) The processor may only process personal data in accordance with the controller's instructions, unless the processor is obliged to process the data in a different way under Union or Member State law to which the processor is subject (e.g. investigations by law enforcement or state security authorities); in such a case, the processor shall notify the controller of these legal requirements prior to processing, unless the law in question prohibits such notification on grounds of important public interest (Art. 28 para. 3 sentence 2 lit. a GDPR). An instruction is a written or electronic order from the controller (text form in accordance with § 126b BGB) that is directed at a specific handling of personal data by the processor. The instructions are generally conclusively defined by the service agreement, the services of the processor and this agreement. Instructions that are not provided for in this list shall be treated as a request for a change of service. If the controller issues individual instructions regarding the handling of personal data that go beyond the contractually agreed scope of services, the resulting costs shall be borne by the controller. In the event that it is impossible or unreasonable to comply with certain instructions, the Processor shall inform the Controller as soon as possible. In this case, the Processor may, notwithstanding § 2 (2), request exemption from the instruction.
(5) The processor shall inform the controller immediately if it believes that an instruction violates or could violate data protection regulations. The Processor shall be entitled to suspend the

implementation of the relevant instruction until it is confirmed or amended by the Controller. The processor is entitled to suspend or terminate the account if this is necessary, taking into account the seriousness of the breach.
(6) Changes to the object of processing with procedural changes must be jointly agreed and documented. The Processor may only provide information to third parties or the data subject with the prior express written consent of the Controller, unless the provision of information is provided for by law, in particular in the case of Section 3 (4) of this Agreement. The processor shall use the personal data for the contractually agreed purposes and is not entitled to pass them on to third parties. Copies and duplicates shall not be made without the knowledge of the controller. This does not apply to backup copies insofar as they are necessary to ensure proper data processing.
(7) The controller shall maintain the record of processing activities within the meaning of Art. 30 (1) GDPR. At the request of the controller, the processor shall provide the controller with information for inclusion in the register, unless the controller is able to obtain this information itself. The processor shall keep a record of all categories of processing activities carried out on behalf of the controller in accordance with the requirements of Art. 30 (2) GDPR.
(8) The processing of personal data on behalf of the controller takes place on the territory of the European Union and in the third countries listed in Annex 2 “Sub-processors”. Processing in third countries is only permitted if it is ensured that the level of protection guaranteed by the GDPR is not undermined, taking into account the requirements of Chapter V of the GDPR. The basic requirements for the lawfulness of the processing remain unaffected.

§ 4 Compliance with mandatory legal obligations by the processor

(1) The processor shall ensure that the persons authorized to process the personal data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality.
(2) The contracting parties shall support each other in proving and documenting their accountability with regard to the principles of proper data processing, including the implementation of the necessary technical and organizational measures (Art. 5 (2), Art. 24 (1) GDPR), insofar as they are not in a position to do so themselves with the means at their disposal.

(3) The processor shall appoint a data protection officer, insofar as this is required in accordance with Art. 37 GDPR. The contact details can be found in Annex 3 “Contact and communication”.

§ 5 Technical and organizational measures and their control

(1) The contracting parties agree on the specific technical and organizational security measures set out in Annex 1 “Technical and Organizational Measures” to this Agreement.
(2) Technical and organizational measures are subject to progress. In this respect, the processor is permitted to implement alternative adequate measures. In doing so, the security level of the measures specified in Annex 1 “Technical and organizational measures” must not be undercut.
(3) The Processor shall provide the Controller with the information from Section 9 of this Agreement that is required to demonstrate compliance with the provisions of this Agreement and the statutory requirements.
(4) The Processor shall provide the Controller with all information necessary for the assessment of the consequences of the intended processing operations for the protection of the data (data protection impact assessment within the meaning of Art. 35 GDPR) and shall support the Controller in any prior consultation with the supervisory authority pursuant to Art. 36 GDPR with the means at its disposal. However, information will only be provided to the extent that the controller is unable to obtain it themselves.
(5) The processor shall take all necessary measures to safeguard the data and the security of the processing, in particular also taking into account the state of the art, and to minimize possible adverse consequences for data subjects.

§ 6 Notification of breaches by the processor

The processor shall inform the controller immediately in the event of serious disruptions to its operations, suspected breaches of this agreement and statutory data protection provisions, breaches of such provisions or other irregularities in the processing of the controller's personal data. This applies in particular with regard to the reporting obligation pursuant to Art. 33 para. 2 GDPR and corresponding obligations of the controller pursuant to Art. 33 and Art. 34 GDPR. The processor assures to support the controller appropriately, if necessary, in its obligations

under Art. 33 and 34 GDPR. The Processor may only carry out notifications for the Controller pursuant to Art. 33 or 34 GDPR following prior instruction in accordance with § 3 of this Agreement.

§ 7 Deletion and return of data

(1) Data carriers and data records provided shall remain the property of the controller.
(2) After closure of the account or earlier at the request of the controller, but at the latest upon termination of the service agreement, the processor shall destroy all documents, processing and usage results and databases (as well as copies or reproductions made thereof) in connection with the contractual relationship that have come into its possession within a period of 7 days. The same applies to test and scrap material. The deletion will be confirmed to the person responsible upon request.
(3) The processor may retain documentation and information that serves as proof of proper data processing in accordance with the respective retention periods until the end of the retention period, even beyond the end of the contract. Alternatively, he may hand them over to the controller at the end of the contract in order to relieve him. The obligations under paragraph 2 shall apply to the personal data stored in accordance with sentence 1 after the end of the retention period.

§ 8 Subcontractors

(1) The Processor is granted general authorization to use other processors (subcontractors) at any time. The subcontractors currently engaged for the performance of this Agreement are described in detail in Annex 2 “Subprocessors”. The Processor shall inform the Controller immediately of any changes regarding the involvement or replacement of subcontractors. The controller may object to such changes in accordance with Art. 28 para. 2 sentence 2 GDPR. The objection must be lodged in accordance with Annex 3 “Contact and communication” and within a period of two weeks from notification (Section 187 (1) BGB). The controller undertakes to lodge the objection in good faith only if there are serious data protection concerns. Once the objection has been effectively lodged, the controller has the right to terminate the commissioned processing without notice within 30 days of the objection. In the event of an objection, the processor may also terminate the commissioned processing at its own discretion. The termination must be made in accordance with Annex 3 “Contact and communication”.

(2) Services provided by subcontractors within the meaning of this provision shall not include services that the Processor uses from third parties as a purely ancillary service to support the execution of the order and which therefore do not directly relate to the provision of the main service. These include - but are not limited to - postal, transportation and shipping services, cleaning services, security services, telecommunications services, user services, maintenance and other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the processor is obliged to make appropriate and legally compliant contractual agreements and to take control measures to ensure the protection and security of the controller's personal data, even in the case of outsourced ancillary services.
(3) If subcontractors are engaged by the Processor, the Processor shall ensure that its contractual agreements with the subcontractor are designed in such a way that the level of data protection at least corresponds to the agreement between the Controller and the Processor and that all contractual and legal requirements are observed; this applies in particular with regard to the use of appropriate technical and organizational measures to ensure an appropriate level of security of the processing. If subcontractors in third countries are involved, the processor shall ensure that the additional requirements of Art. 44 et seq. GDPR are fulfilled.
(4) If the subcontractor fails to comply with its obligations under data protection law, the processor shall be liable to the controller for the subcontractor's compliance with its obligations.

§ 9 Data protection control

The Processor undertakes to provide annually, upon request by the Controller, the information required to demonstrate compliance with the obligations set out in Art. 28 GDPR, in particular the implementation of and compliance with the technical and organizational measures in accordance with § 5 of this Agreement, on a document basis, insofar as the Controller cannot obtain this information itself and it is available to the Processor. For this purpose, the Controller may request a current audit report or current certifications. Controls going beyond this are only possible by appointment and will be charged to the Controller based on the additional effort. Should a supervisory authority inspect the Processor due to culpable conduct on the part of the Controller, the Controller shall bear the personnel and material costs incurred for this.

§ 10 Other provisions

(1) Should the personal data of the controller be jeopardized by seizure or confiscation, by insolvency or composition proceedings or by other events or measures of third parties, the processor shall inform the controller immediately, unless he is prohibited from doing so by court or official order. In this context, the Processor shall immediately inform all competent bodies that the decision-making authority over the data lies exclusively with the Principal as the Controller.
(2) The contracting parties agree that the defense of the right of retention by the processor within the meaning of Section 273 BGB (German Civil Code) is excluded with regard to the personal data to be processed and the associated data carriers.
(3) The Parties agree that any support services under this Agreement shall be provided by the Processor to the extent reasonably expected.

§ 11 Final provisions

(1) The Processor may amend or replace this Agreement with two weeks' notice. The Controller shall be notified of amendments or replacements to the Agreement by email or in its account. The Controller shall have an extraordinary right of termination, which it may exercise within 30 days of notification. The extraordinary termination must be made in accordance with Annex 3 “Contact and communication”.
(2) Should individual provisions of this agreement be invalid or unenforceable, this shall not affect the validity of the remaining provisions. The invalid or unenforceable provision shall be replaced by a valid and enforceable provision whose effects come closest to the objective pursued by the contracting parties with the invalid or unenforceable provision. The above provisions shall apply accordingly in the event that the agreement proves to be incomplete.
(3) German law shall apply. The place of jurisdiction is, as far as permissible, Berlin.

Annex 1 “Technical and Organizational Measures”

Section 5 of the agreement on order processing refers to this appendix to specify the technical and organizational measures.

§ 1 Technical and organizational security measures

The contractual partners are obliged to implement suitable technical and organizational measures in such a way that the processing of personal data is carried out in accordance with the legal requirements and the protection of the rights of the data subject is guaranteed in an appropriate form.

§ 2 Internal organization of the processor

The processor shall design its internal organization in such a way that it meets the special requirements of data protection. In particular, measures shall be taken that are appropriate depending on the type of personal data or categories of data to be protected.

§ 3 Specification of the individual measures

The following measures are defined in detail, which serve to implement the requirements of Art. 32 GDPR:

Nr.	Confidentiality (Art. 32 para. 1 lit. b GDPR)	Implementation of measures
1	**Entry control** Unauthorized persons must be denied access to data processing systems that are used to process personal data.	● Access to offices only by or accompanied by authorized persons, ● Access control system to offices using key concept (door security, entry only with key, documented key allocation), ● Storage of confidential documents exclusively under lock and key in lockable, solid cabinets.
2	**Access control** Data processing systems must be prevented from being used by unauthorized persons.	● Use of state-of-the-art encryption methods, ● Password procedures and password protection through mandatory use of a web-based password manager, ● Password change using a strong password and 90-day cycle, ● two-factor authentication, ● Personal and individual user log-in when logging into the system or company network, ● Obligation to lock the work devices, ● Creation of a user master data record for each

		user, ● IP-restricted access to servers, ● Authorization concept for digital access options. Additional home office regulations: ● The workstation is chosen so that family members or visitors cannot look at the notebook or paper documents ● There is a clean-desk policy at the end of the working day ● Care is taken to ensure that telephone conversations are not overheard by unauthorized persons (e.g. open window, other video conference in progress)
3	**Data access control** Ensuring that those authorized to use a data processing system can only access the personal data subject to their access authorization and that this data cannot be read, copied, changed or removed without authorization during processing.	● Demand-oriented design of the authorization concept and access rights, ● Logging, ● regular evaluation of log files, ● Automated 24/7 monitoring of logs, ● Use of state-of-the-art encryption methods.
Nr.	**Integrity (Art. 32 para. 1 lit. b GDPR)**	**Implementation of measures**
4	**Transfer control** It must be ensured that personal data cannot be read, copied, altered or removed without authorization during electronic transmission or during their transport or storage on data carriers, and that it is possible to check and determine to which bodies personal data are to be transmitted by data transmission devices.	● Transmission and transfer under 256-bit SSL as well as TLS 1.2 and TLS 1.3 encryption, ● Password protection of individual documents with separate password transmission, ● VPN tunnel, ● firewall, ● virus protection, ● Creation of a record of processing activities in accordance with Art. 30 para. 2 GDPR
5	**Input control** It must be ensured that it is subsequently possible to check and determine whether and by whom personal data has been entered, changed or removed from data processing systems.	● Traceability and documentation of data management is ensured by logging systems.
Nr.	**Availability and resilience (Art. 32 para. 1 lit. b GDPR)**	**Implementation of measures**
6	**Availability control** It must be ensured that personal data is protected against accidental destruction or loss.	● Daily backup procedure, ● mirroring of hard disks at the subcontracted processor (RAID procedure), ● uninterruptible power supply at the sub-processor (UPS), ● Firewall and virus protection at the processor and sub-processor, ● Emergency plan, ● fire alarm system.

Nr.	Confidentiality	Implementation of measures
7	**Separation control** It must be ensured that personal data personal data collected for different purposes can be processed separately.	● Multi-client capability of the software, ● Separation of functions between production/test, ● Development and test systems are operated exclusively with test data.
8	**Order control** It must be ensured that personal data processed on behalf of the controller can only be processed in accordance with the controller's instructions.	● Delimitation of authority between controller and processor through clear contract design with delimitation of responsibilities between controller and processor, ● Clear definition of instructions through text form requirement, ● Regulation of the use of subcontracted processing, ● Obligation of employees to maintain data secrecy, ● appointment of a data protection officer, training of employees with regard to compliance with data protection and data security.

A procedure must be established that enables the contracting parties to regularly review, assess and evaluate the effectiveness of the technical and organizational measures used (Art. 32 para. 1 lit. d) GDPR).

Annex 2 “Subprocessors”

§§ Sections 3 and 8 of the agreement on order processing refer to this appendix to specify the subcontractors.

Subcontractor	Company headquarters	Location	Processing location(s)	Purpose / Applicable service	Applicable data protection law
“Brevo” (Sendinblue GmbH)	Köpenicker Straße 126, 10179 Berlin	Germany	Germany	E-mail service provider We use Brevo to send confirmation emails and confirmation text messages as soon as an appointment has been booked, postponed or canceled. Data transmitted: Name, e-mail address, e-mail content, telephone number, SMS content	GDPR, fulfillment of contract acc. to Art. 6, (1) lit. b
Open Telekom Cloud (Telekom Deutschland GmbH)	Landgrabenweg 151, 53227 Bonn	Germany	Germany Netherlands	Hosting	GDPR, fulfillment of contract acc. to Art. 6, (1) lit. b

Annex 3 “Contact and communication”

§§ Sections 4 and 8 of the agreement on order processing refer to this appendix.

Contact details of the data protection officer of the processor:
Zeeg GmbH, Data Protection Officer, Friedrichstraße 114a, 10117 Berlin, legal@zeeg.me

Special communication channels
The objection pursuant to Section 8 (1) of this agreement must be addressed to the data protection officer of the processor (legal@zeeg.me).
The processor reserves the right to fulfill its information obligations, in particular pursuant to § 8 para. 1 and § 11 para. 1 of this agreement, by posting notifications in the controller's account.
Extraordinary termination by the Controller on the basis of Section 2 (2), Section 8 (1) and Section 11 (1) of this Agreement must be sent to legal@zeeg.me.

Signatures

Customer

Signature: _____

Company: _____

Name: _____

Title: _____

Date: _____

Processor

Signature: 

Company: Zeeg GmbH

Name: Florian Horbach, Mohammad Moghaddas

Title: Managing Directors

Date: 06/20/2025