
Wandelbots Data Processing Agreement

by and between

Product Customer as defined in the Wandelbots General Terms and Conditions and underlying order

- Controller -

and

Wandelbots GmbH
Rayskistraße 25
01219 Dresden/Germany

- Processor -

about a commissioned processing in the sense of Art. 28 para. (3) of the General Data Protection Regulation (GDPR).

Preamble

This Data Processing Agreement outlines the obligations of the parties regarding data protection resulting from the processing described in detail in the [Wandelbots General Terms and Conditions](#) and the underlying order(s) ("Agreement").

The terms of this Data Processing Agreement shall apply to all activities related to the Agreement in which employees of the Processor or third parties engaged by the Processor process personal data ("Data") on behalf of the Controller.

If not specifically set out otherwise in this Data Processing Agreement, the definitions from the Agreement shall also apply to this Data Processing Agreement.

§ 1 Subject matter, duration and specification of the processing.

The subject matter of the commission, the type and purpose of the processing and a list of the categories of data and groups of persons concerned are set out in Annex 1 to this Data Processing Agreement.

§ 2 Scope of application and responsibility

1. The Processor shall process personal data on behalf of the Controller. This includes activities which are specified in Annex 1. Within the scope of this Data Processing Agreement, the Controller shall be solely responsible for compliance with the statutory provisions of the data protection laws, in particular for the lawfulness of the transfer of data to the Processor as well as for the lawfulness of the data processing ("controller" within the meaning of Art. 4 No. 7 GDPR).
2. The instructions shall initially be determined by the terms of this Data Processing Agreement and the Agreement and may thereafter be amended, supplemented or replaced by the Controller in writing or in an electronic format (text form) to the body designated by the Processor by means of individual instructions (individual instructions). Instructions not provided for in this Data Processing Agreement and the Agreement shall be treated as a change request. Verbal instructions shall be confirmed immediately in writing or in text form.

§ 3 Obligations of the Processor

1. The Processor may only process data of data subjects within the scope of the order and the Controller's instructions, unless there is an exceptional case within the meaning of Art. 28 para (3) a) GDPR. The Processor shall inform the Controller without undue delay if it is of the opinion that an instruction violates applicable laws. The Processor may suspend the implementation of the instruction until it has been confirmed or amended by the Controller.
2. The Processor shall designate the persons listed in Annex 2 as contact persons of the Processor authorized to give instructions.
3. The Processor shall organize its internal organization within its area of responsibility in such a way that it meets the special requirements of data protection. He shall take technical and organizational measures for the adequate protection of the Controller's data that meet the requirements of the Basic Data Protection Regulation (Art. 32 GDPR). The Processor shall take technical and organizational measures to ensure the confidentiality, integrity, availability and resilience of the systems and services in connection with the Processing on a permanent basis. It shall document this for the time of conclusion of this Data Processing Agreement in the attached Annex 3. The Controller confirms that it is aware of these technical and organizational measures. The Controller shall be responsible for ensuring that these measures provide an appropriate level of protection for the risks of the data to be processed. The Processor reserves the right to change the security measures taken, but it must be ensured that the contractually agreed level of protection is not undercut.
4. The Processor shall support the Controller within the scope of its possibilities in fulfilling the requests and claims of data subjects pursuant to Chapter III of the GDPR and in complying with the obligations set out in Articles 33 to 36 of the GDPR.
5. The Processor shall ensure that the employees involved in the processing of the Controller's data and other persons working for the Processor are prohibited from processing the data outside the scope of the instructions. Furthermore, the Processor warrants that the persons authorized to process the personal data have committed themselves to confidentiality or are subject to an appropriate legal duty of confidentiality. The confidentiality/confidentiality obligation shall continue to exist after termination of the order.
6. The Processor shall inform the Controller without delay if it becomes aware of any violations of the Controller's personal data protection.

7. The Processor shall take the necessary measures to secure the data and to mitigate any possible adverse consequences for the persons concerned and shall consult with the Controller without delay in this regard.
8. The Processor shall ensure that it complies with its obligations under Article 32 para. (1) No. (d) GDPR to implement a procedure for the regular review of the effectiveness of the technical and organizational measures to ensure the security of the processing.
9. The Processor shall correct or delete the contractual data if the Controller instructs the persons named in Annex 2 to do so and this is covered by the scope of instructions. If it is not possible to delete the data in accordance with data protection or to restrict the data processing accordingly, the Processor shall undertake the destruction of data carriers and other materials in accordance with data protection on the basis of an individual order by the Controller or shall return these data carriers to the Controller, unless already agreed in the Agreement.
10. In special cases to be determined by the Controller, data shall be stored or handed over. However, the parties shall conclude a separate contract for this purpose, which shall be separate from the provisions of this Data Processing Agreement.
11. Data, data carriers and all other materials shall be either surrendered or deleted at the request of the Controller after the end of the Agreement.
12. In the event of a claim against the Controller by a data subject with regard to any claims under Art. 82 of the GDPR, the Processor undertakes to support the Controller in defending the claim to the extent possible.
13. If the Controller has to conduct a data protection impact assessment pursuant to Art. 35 of the GDPR, the Processor shall support the Controller with all possible and reasonable measures. As a support measure, the Processor shall forward to the Controller in particular all information available to it that is required for the data impact assessment pursuant to Art. 35 of the GDPR and shall support the Controller in any consultation with the competent supervisory authority that may be required.
14. The Processor shall name its data protection officer to the Controller in Annex 2 to this Data Processing Agreement. A change of the data protection officer shall be notified to the Controller in text form without undue delay. The Processor shall ensure compliance with the requirements of Art. 28 GDPR both in the selection of the person of the data protection officer and in the monitoring of his activities as data protection officer.

§ 4 Duties of the Controller

1. The Controller shall inform the Processor immediately and in full if it discovers errors or irregularities in the results of the order with regard to data protection provisions.
2. The Controller shall ensure that no special categories of personal data within the meaning of Art. 9 para. (1) of the GDPR are transmitted to the Processor at any time.
3. In the event of a claim against the Processor by a data subject with regard to any claims under Article 82 of the GDPR, the Controller undertakes to support the Processor in defending the claim to the extent possible.
4. The Controller shall name to the Processor in Annex 2 to this Data Processing Agreement its contact persons authorized to issue instructions for data protection issues arising within the scope of the Data Processing Agreement.

§ 5 Remuneration

1. The Controller shall owe the Processor reasonable remuneration for the expenses incurred by the Processor in connection with the fulfillment of the obligations under § 3 items 4, 9, 12 and 13 of this Data Processing Agreement on the basis of the hourly rates customary for this.
2. If the parties have agreed on an hourly rate-based remuneration in the Agreement, the agreed hourly rate shall be deemed to be reasonable within the meaning of Section 1 above.

§ 6 Requests from affected persons

1. If a data subject approaches the Processor with requests for correction, deletion or information, the Processor shall refer the data subject to the Controller, provided that an assignment to the Controller is possible according to the data subject's information. The Processor shall immediately forward the request of the data subject to the Controller. The Processor shall support the Controller within the scope of its possibilities upon instruction as far as agreed.
2. The Processor shall not be liable if the request of the person concerned is not answered by the Controller, not answered correctly or not answered in due time.

§ 7 Compliance Measures

1. The Processor shall provide the Controller with evidence of compliance with the obligations set out in this Data Processing Agreement by suitable means.
2. If, in individual cases, inspections by the Controller or an inspector commissioned by the Controller are necessary, these shall be carried out during normal business hours without disrupting the course of operations after notification, taking into account a reasonable lead time. The Processor may make such inspections dependent on prior notification with a reasonable lead time and on the signing of a confidentiality agreement with regard to the data of other Controllers and the technical and organizational measures that have been set up. If the auditor commissioned by the Controller is in a competitive relationship with the Processor, the Processor shall have a right of objection against the auditor.
3. Should a data protection supervisory authority or another sovereign supervisory authority of the Controller carry out an inspection, paragraph 2 shall apply accordingly in principle. It shall not be necessary to sign a confidentiality agreement if this supervisory authority is subject to professional or statutory confidentiality where a violation is punishable under applicable criminal law

§ 8 Term

1. The term of this Data Processing Agreement shall be based on the term of the Agreement. However, the confidentiality obligations set out in the Agreement shall continue to apply beyond the period of termination.

§ 9 Sub Contractors (sub-processors)

1. The use of subcontractors as sub-processors shall be permitted within the scope of the following provisions.
2. A subcontractor relationship relevant in this sense shall exist if the Processor commissions further Processors to perform all or part of the service agreed in the contract. The Processor shall conclude agreements with these third parties to the extent necessary to ensure appropriate data protection and information security measures.
3. The contractually agreed services or partial services shall be performed with the involvement of the subcontractors listed in Annex 4.
4. The Controller agrees that the Processor may involve further subcontractors in the current contractual relationship or replace existing subcontractors.
5. The Processor shall inform the Controller thereof prior to calling in or replacing the subcontractors via electronic format (text form), for example via email or via updating the version of this Data Processing Agreement on wandelbots.com. The Controller may object to the change within a period of two weeks to the person authorized to give instructions named by the Processor in Annex 2. In doing so, the Controller shall state the essential reasons which prevent the Processor from calling in or replacing the subcontractor. If no objection is made within the period, the change shall be deemed to have been approved. If there is an important reason and

if a mutually agreeable solution cannot be found between the parties, the Controller shall be granted a special right of termination.

6. If the Processor places orders with subcontractors, it shall be incumbent upon the Processor to transfer its data protection obligations under this Data Processing Agreement to the subcontractor.
7. If the Processor intends to use subcontractors who intend to transfer data to a third country within the meaning of Article 44 of the GDPR, the Processor shall ensure that the requirements of Articles 44 to 50 of the GDPR are met by the subcontractor. Furthermore, the Processor shall expressly inform the Controller of this.
8. Services which the Processor uses from third parties as a purely ancillary service in order to carry out the business activity are not to be regarded as subcontractor relationships within the meaning of the paragraphs. This includes, for example, cleaning services, pure telecommunication services without concrete reference to services which the Processor provides for the Controller, postal and courier services, transport services or guarding services. The Processor is nevertheless obliged to ensure that appropriate precautions and technical and organizational measures have been taken to ensure the protection of personal data, even in the case of ancillary services provided by third parties. The maintenance and servicing of IT systems or applications constitutes a subcontracting relationship requiring consent and commissioned processing within the meaning of Art. 28 GDPR if the maintenance and testing concerns such IT systems that are also used in connection with the provision of services for the Controller and personal data processed on behalf of the Controller can be accessed during the maintenance.

§ 10 Liability

1. The Controller and the Processor shall be liable vis-à-vis affected persons in accordance with the provisions of Article 82 of the GDPR.
2. In the relationship between the Processor and the Controller, however, liability shall be limited to the maximum liability limits set out in the Agreement.

§ 11 Miscellaneous

1. Should the Controller's data at the Processor be endangered by attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties, the Processor shall immediately inform the Controller thereof. The Processor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with the Controller as the "controller" within the meaning of GDPR.
2. Amendments and supplements to this Data Processing Agreement and all its components - including any warranties of the Processor - shall require a written agreement, which may also be in an electronic format (text form), and the express indication that it is an amendment or supplement to the terms of this Data Processing Agreement. This shall also apply to any waiver of this formal requirement.
3. In the event of any contradictions, the provisions of this Data Processing Agreement shall take precedence over the provisions of the Agreement. Should individual parts of this Data Processing Agreement be invalid, this shall not affect the validity of the rest of this Data Processing Agreement.
4. German law shall apply.
5. The attached Annexes 1 to 4 are the subject matter of this Data Processing Agreement and form an integral part thereof.

Annex 1 to the Data Processing Agreement

A) Subject of the order

Providing the support on the basis of the Service Level Agreement (SLA) with potential possibility to access personal data of the Controller towards whom support is to be provided and without excluding the possibility that these data have to be processed in the individual support case.

B) Nature and purpose of the data processing operations, as well as the categories of data and the persons concerned thereby

The processing may regularly include the following:

Type of data categories	Type and purpose of the data processing of these data	Categories of the persons affected thereby
Contact Data	Communication about a service case	Employees of the Controller
Software Usage Data	Troubleshooting software usage	Employees of the Controller
Additional Data provided by the Controller	Troubleshooting software usage	Employees and Customers of the Controller

Annex 2 to the Data Processing Agreement

Persons authorized to give instructions to the Processor are:

datenschutz@wandelbots.com

The data protection officer of the Processor is:

Richard Bode Attorney at Law
R.echt Bode Rechtsanwaltskanzlei
Maxstraße 11
01067 Dresden/Germany
Mail: datenschutz@wandelbots.com

Authorized persons of the Controller are:

The persons named in the order form.

Annex 3 to the Data Processing Agreement

Confidentiality according to Art. 32 para. 1 lit. a) GDPR

Entry control

Technical measure	Organizational measure
Alarm system	Key control / list
Chip card / transponder	Care in personnel selection
Locking system	Employee badges
Security locks	

Access control

Technical measures	Organizational measures
Login function: User name + password	Creation of user profiles
Intrusion detection systems	Management of authorizations
Firewall	Centralized password assignment
Anti-virus software: Server Controllers Mobile Devices	Policies: "Secure Password" "Delete / Destroy" "Clean desk" General data protection / security
Mobile Device Management	Mobile Device Policy
Encryption: Data media Smartphones notebooks / tablets	
autom. desktop lock	

Admission control

Technical measures	Organizational measures
Document destruction Document shredder (min. level 3) ext. Document shredder (DIN 32757)	Authorization concepts
Physical deletion of data carriers	Administration of user rights by administrators
Logging of accesses during input Change Deletion of data	minimum number of administrators

Separation control

Technical measures	Organizational measures
Separation of production and test environment	Control via authorization concepts
Physical separation Systems Databases Data carriers Definition of database rights	

Pseudonymization

Technical measures	Organizational measures
Separation of assignment data and storage in separate systems	Internal instructions to anonymize / pseudonymize personal measures After transfer After expiration of the legal deletion period

Integrity

Control of disclosure

Technical measures	Organizational measures
Encryption E-mail Encrypted connection (https)	Process overview of regular retrieval transmission
Virtual Private Network	Personal handover (w. protocol)
Logging Access Retrieval	Documentation of data recipients Duration of transfer Deletion periods
Secure transport containers	Care in transport selection
Signature procedure	Transfer in anonymized / pseudonymized form

Input control

Technical measures	Organizational measures
Logging Input Change Deletion	Traceability of data through Input Change Deletion via individual user names
Viewing of logs	Overview of data processing programs
	Assignment of rights (authorization concept) Input Change Deletion
	Responsibility for deletion

Availability and resilience acc. to Art. 32. para. 1 lit. b) GDPR

Availability control

Technical measures	Organizational measures
Fire & smoke detection systems	Existence of an IT emergency plan
Server room Fire extinguishers Temperature & humidity meters Protective sockets Video transmission Alarm signalling	Storage of security media outside the server room No sanitary connections inside or outside the server room Separate partitions
RAID system / hard disk mirroring	Backup & recovery concept (form.) Regular tests
Uninterruptible power supply	

Procedures for regular review, assessment and evaluation according to Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR

Data protection management

Technical measures	Organizational measures
Software solutions in use	Data protection officer (ext.)
central documentation of all procedures and regulations on data protection for employees (after authorization)	IT security officer (int.)
At least annual review of technical protection measures	Employees trained in Data secrecy Awareness (at least annually)
	DSFA is performed as required
	Formalized process for handling information requests
	Information requirements

Incident response management

Technical measures	Organizational measures
Firewall (regularly updated)	Security incidents Data mishaps
Spam filter (regular updating)	Documented procedure
Virus scanner (regular updates)	Documentation process
Intrusion Detection System (IDS)	Involvement of DPO
Intrusion Prevention System (IPS)	Involvement of ISB formal follow-up process

Data protection-friendly default settings in accordance with Art. 25 (2) GDPR

Technical measures	Organizational measures
As much personal data is collected as required for the respective purpose	
Technical measures for revocation	

Processing control (outsourcing to third parties)

Technical measures	Organizational measures
	Selection of Processor Verification of security measures Due diligence for data protection
	Conclusion of the GCU written instructions Control rights Use of additional subcontractors
	Duties of the Processor Reference to data secrecy Appointment of a DPO
	In case of ongoing cooperation: regular review of the level of protection

Annex 4 to the Data Processing Agreement

The Processor uses the following subcontractors at the time of the conclusion of the Data Processing Agreement:

Subcontractor	Services performed	Intended or necessary data processing in a third country
If the Controller has acquired Wandelbots Products from one of our authorized Partners, this Partner, as outlined in the underlying order for acquiring the Wandelbots Products, is the Processor's subcontractor	First Level Support	Only if Partner is located outside the European Union (EU)
Atlassian. Pty Ltd	ticketing and documentation tool for support requests and supply chain	Generally, data are hosted in the European Union (EU). Otherwise, EU Standard Contractual Clauses apply.
Swyx (powered by Telekom)	managing phone system	No