Data Processing Agreement

according to EU GDPR

Version 1.1

Valid from: November 1, 2020

Hallo Welt! GmbH | Maximilianstraße 9 | 93047 Regensburg | +49 941 660 80 0

Between

Company

Address

Country

(the Controller) hereinafter referred to as „the Client“

and

Hallo Welt! GmbH
Maximilianstraße 9, 93047 Regensburg, Germany (the Processor)
hereinafter referred to as „the Supplier“,

hereinafter collectively referred to as „the Parties".

the following agreement is made for order processing according to article 28 EU GDPR:

1. Subject matter and duration of the Order or Contract

1.1 Subject matter

The Subject matter of the Order or Contract results from the Service Agreement, which is referred to here (hereinafter referred to as Service Agreement).

1.2 Duration

The Contract is authorised for an unlimited period, but shall end automatically, i.e. without further declaration by either party, upon termination of the service agreement.

2. Specification of the Order or Contract Details

2.1. Nature and purpose of the intended Collection, Processing or Use of Data

The Supplier is, depending on the order, entrusted with the following services within the scope of his activities:

a) The Supplier provides **technical support**. In the course of this it may be necessary to access the system with a privileged access ("Administrator").

b) The Supplier performs the **software maintenance** of the system. This requires access to the server and the database.

c) The Supplier performs **software development** for the Client. Within the scope of acceptance tests and productive implementation it may be necessary to access the system with a privileged access ("Administrator").

d) In the course of a **migration**, the Supplier transfers data of the Client from external sources into a BlueSpice Wiki. In order to fulfill this task, the Supplier must automatically process the provided data to be migrated with all personal data contained therein and check it manually on a random basis. In doing so, he can gain knowledge of all content that has been made available.

e) The Supplier provides a **cloud service**. To operate and maintain this service it may be necessary to access the cloud instances with a privileged access ("Administrator") or to gain access to the server and data of the cloud instances.

f) The Supplier uses a **ticket system** (EasyRedmine) for order-related communication with the customer.

Further order components are:

_____

The subject of the order is **not** the original use or processing of personal data by the Supplier. In the course of the service provision of the Supplier as a software maintenance service provider in the area of hosting, cloud services, support or administration of server systems of the Client, access to personal data cannot be excluded.

The Supplier is obliged to use the personal data provided to him exclusively for the contractually agreed service. The Supplier is permitted to create intermediate, temporary or duplicate files required for procedural and security reasons for the collection, processing and/or use of personal data in accordance with the performance, provided this does not lead to a change in content. The Supplier is not permitted to make unauthorized copies of the personal data.

The undertaking of the contractually agreed Processing of Data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every Transfer of Data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of the Client and shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled.

2.2. Type of Data

2.2.1. Supplier

The Subject Matter of the collection, processing or use of personal data comprises the following data types/categories (List/Description of the Data Categories):

- Personal Master Data (Key Personal Data): Username, real name
- Communication data: Email
- Login and logout times, action logs and access logs

☐ Other data (e.g. additional profile fields):

_____

2.2.2. Client

The Subject Matter of the collection, processing or use of personal data of the Client comprises the following data types/categories (List/Description of the Data Categories):

- ☐ Personal Master Data (Key Personal Data)
- ☐ Communication data, e.g. phone and email
- ☐ Key Contract Data (Contractual/Legal Relationships, Contractual or Product Interest)
- ☐ Customer History
- ☐ Contract Billing and Payments Data
- ☐ Disclosed Information (from third parties, e.g. Credit Reference Agencies or from Public Directories)
- ☐ Planning and control data
- ☐ Other data: _____

2.3. Categories of Data Subjects

2.3.1. Supplier

The categories of data subjects affected by processing by the provided software include:

- Employees of the Client

- ☐ Other affected persons: _____

2.3.2. Client

The categories of persons affected by the processing in the course of use by the Client include:

- ☐ Customers
- ☐ Potential Customers
- ☐ Subscribers
- ☐ Employees
- ☐ Suppliers
- ☐ Authorized Agents
- ☐ Contact Persons
- ☐ Other: _____

3. Technical and Organizational Measures

Before the commencement of processing, the Supplier shall document the execution of the necessary Technical and Organizational Measures (TOM), set out in advance of the awarding of the Order or Contract, specifically with regard to the detailed execution of the contract, and shall present these documented measures to the Client for inspection. Upon acceptance by the Client, the documented measures become the foundation of the contract. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.

The Supplier shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account (Details in Appendix TOM).

The Technical and Organizational Measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

4. Rectification, restriction and erasure of data

The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Client, but only on documented instructions from the Client. Insofar as a Data Subject contacts the Supplier directly concerning a rectification, erasure, or restriction of processing, the Supplier will immediately forward the Data Subject's request to the Client.

Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Client without undue delay.

5. Quality assurance and other duties of the Supplier

In addition to complying with the rules set out in this Order or Contract, the Supplier shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Supplier ensures, in particular, compliance with the following requirements:

a) Appointed Data Protection Officer, who performs his/her duties in compliance with Articles 38 and 39 GDPR. The Supplier has appointed

Mr. Matthias Haßler, Projekt 29 GmbH & Co. KG

as Data Protection Officer. The Client shall be informed immediately of any change of Data Protection Officer.

b) Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Supplier entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Client, which includes the powers granted in this contract, unless required to do so by law.

c) Implementation of and compliance with all Technical and Organizational Measures necessary for this Order or Contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR (details in Appendix TOM).

d) The Client and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.

e) The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Order or Contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of this Order or Contract.

f) Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract data processing by the Supplier, the Supplier shall make every effort to support the Client.

g) The Supplier shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

h) Verifiability of the Technical and Organizational Measures conducted by the Client as part of the Client's supervisory powers referred to in item 7 of this contract.

6. Subcontracting

Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Supplier shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

The Supplier may commission subcontractors (additional contract processors) only after prior explicit written or documented consent from the Client.

The Client agrees to the commissioning of the subcontractors listed in Appendix SUB on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

Outsourcing to subcontractors or changing the existing subcontractor are permissible when:

- The Supplier submits such an outsourcing to a subcontractor to the Client in writing or in text form with appropriate advance notice; and
- The subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

The transfer of personal data from the Client to the subcontractor and the subcontractors commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

If the subcontractor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

Further outsourcing by the subcontractor requires the express consent of the main Client (at the minimum in text form); All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

7. Supervisory powers of the Client

The Client has the right, after consultation with the Supplier, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Supplier in his business operations by means of random checks, which are ordinarily to be announced in good time.

The Supplier shall ensure that the Client is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR**.** The Supplier undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

Evidence of such measures, which concern not only the specific Order or Contract, may be provided by

- Compliance with approved Codes of Conduct pursuant to Article 40 GDPR;
- Current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor).

The Supplier may claim remuneration for enabling Client inspections.

8. Communication in the case of infringements by the Supplier

The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.

b) The obligation to report a personal data breach immediately to the Client.

c) The duty to assist the Client with regard to the Client's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.

d) Supporting the Client with its data protection impact assessment.

e) Supporting the Client with regard to prior consultation of the supervisory authority.

The Supplier may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of the Supplier.

9. Authority of the Client to issue instructions

The Client shall immediately confirm oral instructions (at the minimum in text form).

The Supplier shall inform the Client immediately if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

10. Deletion and return of personal data

Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the Service Agreement, the Supplier shall hand over to the Client or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

Documentation which is used to demonstrate orderly data processing in accordance with the Order or Contract shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods. It may hand such documentation over to the Client at the end of the contract duration to relieve the Supplier of this contractual obligation.

11. Liability

Reference is made to Art. 82 GDPR.

Additionally, the following is agreed upon:

_____

Place, date	Place, date
Signature controller	Signature processor

Appendix TOM - Technical and Organizational measures

Nr.	Area	Description
0	**Organization**	
	How is the implementation of data protection organized?	An external data protection officer is appointed to perform the advisory and control functions arising from the GDPR.
	Please give us the name and contact details of your data protection officer.	Matthias Haßler (LL.M.) +49-941-2986930 Projekt 29 GmbH & Co. KG Ostengasse 14 93047 Regensburg, Germany
	In what form are the employees trained on the implementation of the agreed technical and organizational measures that are used for this processing?	The training concept includes data protection instruction at the start of the job as well as constant sensitization through monthly data protection newsletters, specialized web training and personal sensitization by the external data protection officer.
	Are the processing operations documented with regard to data protection law compliance?	Within the framework of the internal directory for processing activities, the data flows are documented and the permissibility of processing and use in accordance with the GDPR is proven.

Nr.	Area	Description
1	**Confidentiality (Art. 32 sec. 1 point b GDPR)**	
1.1	**Building Access Control**	
	How are the buildings where the processing takes place secured from unauthorized access?	The building is equipped with a security locking system.
	How are the rooms/offices where the processing takes place secured against unauthorized access?	The rooms are also secured by the security locking system.
	How are the processing plants protected from unauthorized access?	Yes, through access restrictions such as changing passwords in accordance with BSI and through a selective rights and role concept. Wherever technically feasible, a two factor authentication is used for privileged accounts.
	How are the implemented access control measures checked for suitability?	As part of the controls by the external data protection officer, the access control measures are also reviewed.
1.2	**User Access Control**	
	How is user access allocated?	User access is granted by the IT department as part of the employee onboarding process and only after management approval. Assignment of rights and changes are documented. Access to commercial documents and communication information is protected by passwords.
	How is the validity of user access checked?	An audit of the assigned rights is part of the audits of the measures and is carried out together with the external data protection officer and documented by him.

	How are user accesses incl. application, approval procedures, etc. documented?	The creation and modification of user accesses is documented in the company's own ticket system.
	How is it ensured that the number of administration additions is reduced exclusively to the necessary number and that only professionally and personally suitable personnel are used for this purpose?	The decisions on the allocation of rights strictly adhere to the corresponding specifications, data avoidance and data economy, less is often more here.
	Is it possible to access the systems/applications from outside the company (home workstations, service providers, etc.) and how is the access designed?	Employees can work from their home office. External access to the network is only possible via VPN with appropriate authentication (certificate and password).
1.3	**Password Access Control**	
	How is it achieved that passwords are known only to the respective user?	The passwords are assigned by the respective employees themselves. The strict system default settings force a high password complexity. Passwords are not stored.
	What are the requirements for the complexity of passwords?	The recommendations of the BSI serve as a model for the above-mentioned system settings.
	How is it guaranteed that the user can/must change his/her password on a regular basis?	With reference to the above system settings.
	What organizational arrangements are being taken to prevent unauthorized access to personal data at the workplace?	Training and sensitization of employees. Instruction and regular training on the equipment used.
	How is it ensured that access permissions are granted in a request-friendly and time-limited manner?	See also item Allocation of user access point 1.2; the IT department checks the rights and user structure at regular intervals.

1.4	**Separation control**	
	How is it ensured that data collected for different purposes is processed separately?	Strict separation between CRM, ticket system, and cloud operations.
1.5	**Pseudonymization**	
	What organizational measures have been taken to ensure that the processing of personal data is carried out in accordance with the law?	All persons entrusted with the processing of personal data have been obligated accordingly. A data protection concept is used in the company and is made known to all employees. The training concept includes both data protection instruction at the start of employment and constant sensitization through monthly data protection newsletters, specialized web training and personal sensitization by the external data protection officer. Attention has been drawn to the special features in dealing with pseudonymized data.

Nr.	Area	Description
2	**Integrity (Art. 32 sec. 1 point b GDPR)**	
2.1	**Transfer control**	
	How do you ensure the integrity and confidentiality of the transfer of personal data?	In principle, no data will be passed on to third parties. If this is absolutely necessary for the provision of services, this is done on the basis of a Data Processing Agreement.
	How is the unauthorized outflow of personal data restricted by technical measures?	A strict assignment of rights protects the data from unauthorized access.
2.2	**Input control**	
	What measures are being taken to understand who accessed applications, when and for how long?	Login and logout as well as changes are logged in the systems.
	How is its comprehensible which activities were carried out on the corresponding applications?	Login and logout as well as changes are logged in the systems.
	What measures are taken to ensure that the employees can only process them in accordance with the instructions of the client?	Access control based on the roles/rights concept for proper data processing and storage. Registration and deregistration as well as changes are logged in the systems.
	What measures are taken to ensure that subcontractors also carry out personal data of the client exclusively to the agreed extent?	All subcontractors are subject to the same specifications as the contractor. Corresponding contracts have been concluded. The company's data protection officer is responsible for checking the subcontractors. He is also significantly involved in the selection of the subcontracted companies.

	How is the deletion/blocking of personal data ensured at the end of the retention period with subcontractors?	Determination by contractual obligation, if the purpose no longer applies, deletion of the data is also indicated.

Nr.	Area	Description
3	**Availability and resilience**	
3.1	**Availability control**	
	How is it ensured that the data carriers are protected from elementary influences (fire, water, electromagnetic radiation, etc.)?	Saved data is physically separated from productive data; in addition, the saved data is stored in an external data center. For the cloud service, saved data is located on a separate block storage at the cloud infrastructure service provider.
	What protective measures are used to combat malware and how is their up-to-dateness ensured?	Constantly updated virus scanners and spam filters are used. The systems are regularly updated.
	How do you ensure that data carriers that are no longer needed or defective are properly disposed of?	Physical deletion of functional data carriers and mechanical destruction of defective data carriers before disposal.
3.2	**Recoverability**	
	What organizational and technical measures are taken to ensure the availability of data and systems as quickly as possible, even in the event of damage? (rapid recoverability in accordance with Article 32 (1) point. c GDPR)	Established 2-stage backup procedure. Restoration of the data states of the past 7 days on demand; all local backups can be restored within one hour. Externally backed up data is available again after a maximum of one day. For the cloud service backups are created on an hourly basis. They are kept for 2 days.

Nr.	Area	Description
4	**Procedure for regular review, assessment, evaluation (Art. 32 (1) point d GDPR, Art. 25 (1) GDPR)**	
	What is the regular assessment/ verification procedures to ensure the security of data processing (data protection management)?	The external data protection officer checks regularly, and sometimes unannounced, that the technical and organizational measures are observed.
	How do you react to inquiries or problems (Incident-Response-Management)?	Use of a ticket system (basis EasyRedmine); additional automated monitoring and alerting (Nagios/Zabbix).
	What are the data protection-friendly default settings (Art. 25 para. 2 GDPR)?	No pre-setting by ticking the checkbox; no pre-settings are made when logging into the system; user must enter the login information in each case.
4.1	**Order supervision**	
	What are the procedures for issuing instructions and handling order data processing (data protection management)?	The contract was designed in accordance with the new guidelines for commissioned data processing. The external data protection officer performs corresponding advisory and monitoring duties.

Appendix SUB - List of Subprocessors

Subcontractor	Description
Cloud services	
DigitalOcean, LLC 101 Avenue of the Americas NY 10013, United States	Provision of server infrastructure for cloud services Server location: Frankfurt Datacenter (FRA1), Germany
MailJet SAS 13-13 bis, rue de l'Aubrac 75012 Paris, France	Provision of cloud mail service for cloud services
Hosting	
SaaS Web Internet Solutions GmbH Steinstraße 25 76133 Karlsruhe, Germany	Setup and support of wikis in the hosting environment
netcup GmbH Daimlerstraße 25 D-76185 Karlsruhe, Germany	Provision of servers for hosted wikis Server location: Nürnberg, Germany
Customer service	
Easy Software Ltd. Kemp House, 152-160, City Road EC1V 2NX London, United Kingdom	Provision and operation of ticket system for customer service