DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") specifies the data protection rights and obligations of the parties in connection with the processing of personal data processed by Kubermatic GmbH (hereinafter "**Kubermatic**") on behalf of its customer (hereinafter "**Customer**") under the main agreement ("hereinafter "**Main Agreement**") concluded between the parties.

1. Scope of application

When providing the services in accordance with the Main Agreement, Kubermatic processes personal data which Customer has made available for purpose of providing the services and in respect of which Customer acts as controller in the sense of data protection law ("Customer Data"). In the event of contradictions between this DPA and provisions from other agreements, in particular from the Main Agreement, the provisions of this DPA shall take precedence.

2. Subject matter and scope of the processing / Customer’s authority to issue instructions

2.1. Kubermatic will process the Customer Data exclusively on behalf of Customer and in accordance with Customer's instructions, unless Kubermatic is legally required to process such data under the law of the European Union or a Member State. In such a case, Kubermatic shall inform Customer of these legal requirements prior to processing, unless the law in question prohibits such information on important grounds of public interest.

2.2. The processing of Customer Data by Kubermatic shall be carried out exclusively in the nature, to the extent, and for the purposes specified in Annex 1 to this DPA; the processing shall only concern the types of personal data and categories of data subjects specified therein.

2.3. The duration of the processing corresponds to the term of the Main Agreement.

2.4. Kubermatic is allowed to process Customer Data or have Customer Data processed by sub-processors outside the European Economic Area ("EEA") in accordance with Section 5 of this DPA, if the requirements of Articles 44 to 48 GDPR are fulfilled or if an exception under Art. 49 GDPR exists.

2.5. The instructions are set out in the Main Agreement. Customer is entitled to issue further instructions regarding the nature, scope, purposes and means of processing Customer Data only where such instructions are required by the law of the European Union or a Member State, or by court or administrative order. In all other cases, if Customer issues instructions that go beyond the services agreed in the Main Agreement and this DPA, Customer shall bear the costs and expenses for the execution of such instructions. Before carrying out such instructions, Kubermatic shall inform Customer of the expected costs and await his confirmation. This shall not apply to instructions to refrain from data processing as a whole or to delete individual or all Customer Data or to hand it over to Customer.

2.6. Instructions shall be in writing (email sufficient). Customer will confirm oral instructions in writing or by email.

2.7. Kubermatic shall inform Customer immediately if, in its opinion, an instruction infringes this DPA, the GDPR or other data protection provisions of the European Union or the Member States. Kubermatic is entitled to suspend the execution of such an instruction until Customer confirms the instruction in writing (email sufficient). If Customer insists on the execution of an instruction despite the concerns expressed by Kubermatic, Customer shall indemnify and hold harmless Kubermatic from and against any and all damages and costs incurred by Kubermatic as a result of the execution of Customer's instruction. Kubermatic shall inform Customer of any damages and costs asserted against him and shall not acknowledge any claims of third parties without the consent of Customer and shall either conduct the defense in agreement with Customer or leave it to Customer.

3. Requirements for personnel

3.1. Kubermatic shall obligate all personnel processing Customer Data to maintain confidentiality, unless they are subject to appropriate statutory confidentiality obligations.

3.2. Kubermatic shall ensure that all personnel under his authority who have access to Customer Data only process this data in accordance with this DPA and Customer's instructions, unless they are required to process Customer Data under the law of the European Union or the Member States.

4. Security of processing

4.1. Taking into account the state of the art, the costs of implementation and – as far as known to Kubermatic – the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects, Kubermatic shall implement appropriate technical and organizational measures to ensure a level of security for Customer Data appropriate to the risk.

4.2. Prior to the beginning of the processing of Customer Data, Kubermatic shall in particular implement the technical and organizational measures specified in Annex 2 to this DPA and maintain them for the duration of the Main Agreement and ensure that the processing of Customer Data is carried out in accordance with these measures.

4.3. Customer shall verify the technical and organizational measures implemented by Kubermatic, in particular whether they are also sufficient with regard to circumstances of data processing not known to Kubermatic.

4.4. Since the technical and organizational measures are subject to technical progress, Kubermatic is entitled and obligated to implement alternative, adequate measures in order not to fall below the security level of the measures specified in **Annex 2**. If Kubermatic makes significant changes to the measures set out in **Annex 2**, it shall inform Customer thereof in advance.

5. Use of sub-processors

5.1. Kubermatic uses the sub-processors listed in Annex 3 for the processing of Customer Data. These are deemed to be authorized upon conclusion of this DPA.

5.2. Kubermatic may use further sub-processors to process Customer Data subject to the following conditions:

5.3. Kubermatic shall inform Customer at least 30 days before making use of the further sub-processor in written form (email sufficient) to a contact address specified by Customer for this purpose. Unless Customer raises an objection within 14 days, the use of the further sub-processor shall be deemed to have been authorized.

Such further sub-processors shall be added to **Annex 3.**

5.4. If Customer objects to the use of a further sub-processor, Kubermatic shall be entitled, at its discretion, to continue to provide the services without the rejected sub-processor or to terminate the Main Agreement and this DPA.

5.5. Kubermatic must obligate each sub-processor by means of a written agreement in the same way as Kubermatic is obligated to Customer under this DPA.

5.6. Kubermatic shall be obligated to select and use only those sub-processors who offer sufficient guarantees that the appropriate technical and organizational measures are implemented in such a way that the processing of Customer Data is carried out in accordance with the requirements of the GDPR and this DPA.

6. Rights of data subjects

6.1. Kubermatic shall take all reasonable technical and organizational measures to assist Customer in fulfilling its obligation to respond to requests from data subjects to exercise their rights.

Kubermatic will in particular, within the scope of his possibilities:

6.1.1. inform Customer if a data subject should contact Kubermatic directly with a request to exercise his rights in relation to Customer Data;

6.1.2. provide Customer, upon request, with all information in its possession concerning the processing of Customer Data which Customer requires in order to respond to the request of a data subject and which is not available to Customer himself;

6.1.3. correct, delete or limit the processing of Customer Data without delay at Customer's instruction, insofar as Customer cannot do this himself and this is technically possible for Kubermatic;

6.1.4. to assist Customer, if necessary, to receive Customer Data processed in Kubermatic's sphere of responsibility – as far as technically possible – in a structured, commonly used and machine-readable format, provided that the data subject has a right to data portability with regard to Customer Data.

7. Other obligations of Kubermatic to assist Customer

7.1. Kubermatic shall notify Customer immediately after becoming aware of any Customer Data breach, in particular incidents which lead to the destruction, loss, alteration or unauthorized disclosure of or access to Customer Data. Such notification shall contain a description, if possible, of:

7.1.1. the nature of the Customer Data breach, specifying, where possible, the data categories and approximate number of data subjects concerned;

7.1.2. the possible consequences of the Customer Data breach;

7.1.3. the measures taken or proposed by Kubermatic to remedy the Customer Data breach and, where appropriate, measures to mitigate its possible adverse effects.

7.2. In the event of any Customer Data breach, Kubermatic shall, without delay, take all necessary and reasonable measures to remedy Customer Data breach and, if necessary, to mitigate its possible adverse effects.

7.3. If Customer is obligated to provide information about the processing of Customer Data to a government agency or a third party or to otherwise cooperate with such entity, Kubermatic shall be obligated to support Customer in providing such information or in fulfilling other obligations to cooperate.

7.4. Kubermatic shall assist Customer with its compliance with its obligations under Art. 32 GDPR, to the extent possible considering the information Kubermatic has with respect to Customer’s use of Kubermatic’s services.

7.5. In the event that Customer is obligated to inform supervisory authorities and/or data subjects in accordance with Art. 33, 34 GDPR, Kubermatic shall, insofar as this is possible, assist Customer in complying with these obligations at the latter's request. In particular, Kubermatic is obligated to document all Customer Data breaches, including all related facts, in a manner that enables Customer to prove compliance with any relevant statutory reporting obligations.

7.6. Kubermatic shall support Customer with the information available to him and assist, within reason, in any data protection impact assessment to be carried out by Customer and, if necessary, subsequent consultations with the supervisory authorities in accordance with Art. 35, 36 GDPR.

8. Data deletion and return

8.1. Upon termination of the Main Agreement , Kubermatic shall, upon Customer's instruction, either completely delete all Customer Data or return it to Customer , unless the law of the European Union or a Member State requires the continued storage of Customer Data.

8.2. However, Kubermatic is entitled to keep backup copies of Customer Data for a period of 30 days, insofar as deletion of Customer Data from these backup copies is not required for technical reasons or with regard to Art. 32 GDPR. For this period, the rights and obligations of the parties under this DPA with regard to the backup copies shall continue to apply in deviation from section 2.3.

8.3. Documentation which serves as proof of the orderly and proper processing of Customer Data is to be kept by Kubermatic in accordance with the statutory retention periods beyond the term of this DPA.

9. Audit rights

9.1. Kubermatic shall ensure and regularly evaluate that the processing of Customer Data is carried out in accordance with this DPA, the Main Agreement and Customer's instructions.

9.2. Kubermatic shall document the implementation of the obligations under this DPA in a suitable manner and shall provide Customer with all necessary evidence of Kubermatic's compliance with its obligations under the GDPR and this DPA at Customer's request.

9.3. Customer shall be entitled to audit Kubermatic prior to the start of the processing of Customer Data and regularly during the term of the Main Agreement with regard to compliance with the provisions of this DPA, in particular the implementation of the technical and organizational measures in accordance with Annex 2, either itself or through a qualified auditor subject to appropriate confidentiality obligations; this shall include inspections. Kubermatic shall allow and shall contribute to such inspections by taking all reasonable and appropriate measures; inter alia by granting the necessary access rights and by providing all necessary information.

9.4. The inspections shall not, as far as possible, obstruct or unduly burden Kubermatic in his normal business operations. In particular, inspections at Kubermatic's premises without any specific reason should not take place more than once per calendar year and only during Kubermatic's normal business hours. Customer shall notify Kubermatic of inspections in good time in advance and in writing (email sufficient).

9.5. In accordance with the provisions of the GDPR, Customer and Kubermatic are subject to public controls by the competent supervisory authority. At the request of Customer, Kubermatic shall provide the supervisory authority with the desired information and shall give the supervisory authority or the persons appointed by it the opportunity to carry out audits, including inspections of Kubermatic. In this context, Kubermatic shall grant the competent supervisory authority the necessary rights of access, information and inspection.

10. Liability

Both parties shall be liable in accordance with statutory provisions**.**

11. Miscellaneous

11.1. Amendments and subsidiary agreements to this DPA must be made in writing. This also applies to this written form clause.

11.2. Agreements on the choice of law and place of jurisdiction from the Main Agreement shall apply accordingly to this DPA.

Annex 1 - Purpose, nature and extent of data processing, type of data and categories of data subjects

Purpose of the data processing	Rendering of the Services by the Kubermatic to the Customer, as agreed in the Main Agreement between the parties Processing initiated by Users in the course of their use of or access to the Services Processing to comply with other reasonable and documented instructions provided by the Customer that are consistent with the terms of the Main Agreement.
Nature and scope of data processing	Support Services: Personal Data of Customer's employees issuing Support Services requests ('tickets") may be Processed by Kubermatic for the purposes of administering the Support Services. Kubermatic's personnel may access Customer's instance on a case-by-case basis if requested by the Customer. Online Training Cloud: Customer's employees may participate in training provided by Kubermatic. In such cases, contact details and participation information, including training outcomes, will be processed and used for interaction with the training participant as well as for reporting to the Customer. Professional Services: In the context of consulting, Kubermatic's personnel may access Customer's instance on a case-by-case basis if requested by the Customer.
Type of data	User Account related data such as name, username/ID, contact details, lop and protocol data. Further categories of Personal Data, depending on the Customer's use of the Services.
Categories of data subjects	Employees of the Customer. Further categories of Data Subjects, depending on the Customer's use of the Services.

Annex 2 – Technical and organizational measures

This document describes the requirements and implementation of measures for secure and compliant processing of personal data.

1. Confidentiality

1.1 Entry control

Measures for preventing unauthorized individuals from accessing the premises where personal data are processed:

X	Locked building	X	Locked server rooms with entry control
X	Electronic security locking system	X	Locked server cabinets
X	Mechanical security locking system	X	Documented key issuance

1.2 Access control

Measures for preventing unauthorized individuals from accessing the personal data processed digitally:

X	Personalized user accounts	X	Use of an up-to-date firewall
X	Complex passwords	X	Multifactor access control
X	Central authentication	X	Systems access is logged and monitored
X	Access blocked after five incorrect password entries		

1.3 Usage control

Measures for restricting and monitoring accesses to personal data:

X	Role-based authorization process	X	Protected access to data storage media
X	Authentication with unique username and password	X	Secure destruction of paper documents
X	Logging user access and data processing	X	Encryption of data at rest
X	Allocation of authorizations only after approval by the data owner	X	Minimization of superuser access

1.4 Personal data minimization

Measures to minimize the use of personal data:

X	Processing of personal data restricted to the minimal required for the defined purpose	X	Pseudonymization of personal data whenever feasible

1.5 Separation control

Measures for separating personal data by means of various storage locations or logical separation:

X	Separation of production and test systems	X	Separation of personal data with the data processing systems

2. Integrity

2.1 Transmission control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during transmission:

X	For data in transit required AES-256 encryption.	X	Special protection when physically transporting data storage media
X	The use of private data storage media is prohibited	X	Connections to the infrastructure by employees are encrypted end-to-end

2.2 Input control

Measures to ensure that it is possible to check and establish retrospectively whether and by whom personal data has been processed:

X	Traceability when assigning, changing and deleting user authorizations

2.3 Contractual order control

Measures to ensure that the personal data processing carried out on a subcontracted basis takes place exclusively at the instruction of the Controller:

X	Documentation of processing activities	X	Written agreement with the processor on the data protection minimum standard
X	Careful selection of processors (detailed assessment of provided guarantees)	X	Assuring compliant destruction or return of data upon completion of the assignment
X	No use of processors who have not entered into agreement pursuant to Article 28 GDPR where applicable		

3. Availability and reliability

Measures for protecting personal data against accidental destruction or loss:

X	Regular documented patch management for servers	X	Physically separate redundant data storage or backup data
	Regular documented patch management for endpoint devices		Uninterrupted power supply
X	Mitigate and remediate any confirmed zero-day vulnerabilities	X	Early fire detection in office buildings
X	Recovery procedures are established and tested at least annually		

4. Procedure for routine review, assessment, and evaluation

Measures for monitoring personal data protection and for verifying appropriateness of established technical and organizational measures:

X	Appointment of a data protection officer where required	X	Regular audits by independent third parties
X	Regular documented training of employees involved in personal data processing	X	Regular review of the latest technical standards pursuant to Article 32 GDPR
X	Documented procedure for introducing, modifying, and discontinuing procedures	X	Regular auditing or other suitable verifications of the processors

Annex 3 – Sub-processors

Sub-processor name and location	Description of processing
Amazon Web Services Inc., Seattle, United States Hosting location for Customers in the United States and Canada: United States or Canada Hosting location for European Customers: European Union, e.g., Germany Other optional hosting locations: Australia	VSOC (Virtual Service Operation Center), VPN, monitoring, logging
Freshworks Inc., San Mateo, California, United States US, EEA, IND and AU	Ticket data, requestor/contact data, social data, application integration data,knowledge base data, forum data, report data, call recording, chat messages
Loovent UG, Hamburg, Germany Germany	Marketing and events
Our applicable affiliates: Loodse Inc., State of Delaware, United States US	General support of Services through personnel of such Affiliate (contracting Kubermatic entity)