DATA PROCESSING AGREEMENT FOR DOCKER SERVICES

This Data Processing Agreement for Docker Services ("DPA") forms a part of the software subscription agreement or other written agreement between Docker and Customer ("Agreement") regarding Docker's subscriptions and/or products or services provided by Docker and ordered by Customer (the "Service") in accordance with the Agreement. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

This DPA is an addendum to and forms a part of the Agreement. If any terms of this DPA are inconsistent with the terms of the Agreement, including the exhibits thereto, then the terms of this DPA shall prevail.

DATA PROCESSING TERMS

1. BACKGROUND

1.1 **Purpose.**

This DPA applies to Personal Data provided by Customer and each Data Controller in connection with their use of the Service. It states the technical and organizational measures Docker uses to protect Personal Data that is stored in the production system/technical instance of the Service.

1.2 Application of the Standard Contractual Clauses Document.

If processing of Personal Data involves an International Transfer, the EU Standard Contractual Clauses and/or the UK Standard Contractual Clauses, as the case may be, apply, and as stated in Section 5 and are incorporated by reference.

1.3 Governance.

Except as provided in Section 5.2, Customer is solely responsible for administration of all requests from other Data Controllers. Customer will either (i) bind any other Data Controller it permits to use the Service to the terms of this DPA, or (ii) ensure, through other instruments, including, but not limited to, intra-group agreements, that any other Data Controller it permits to use the Service will adhere to the terms of this DPA.

2. APPENDICES

Customer and its Data Controllers, as applicable, determine the purposes of collecting and processing Personal Data in the Service. Appendix 1 states the details of the processing Docker will provide via the Service under the Agreement. Appendix 2 states the technical and organizational measures Docker applies to the Service, unless the Agreement states otherwise. Appendix 3 defines the applicable modules and options for the EU Standard Contractual Clauses and the UK Standard Contractual Clauses.

3. DOCKER OBLIGATIONS

3.1 Instructions from Customer.

Docker will follow instructions received from Customer (on its own behalf or on behalf of its Data Controllers) with respect to Personal Data, unless they are (i) legally prohibited or (ii) require material changes to the Service. In the event and to the extent the functionality of the Service does not allow Customer, its Data Controllers or authorized users to do so, Docker may correct, block or remove any Personal Data in accordance with Customer's instruction. If Docker cannot comply with an instruction, it will notify Customer (email permitted) without undue delay.

3.2 Technical and Organizational Measures.

(a) Docker will use the appropriate technical and organizational measures to protect all Personal Data.

(b) Docker provides the Service to Docker's entire customer base hosted out of the same Data Center(s) receiving the same Service. Customer agrees Docker may improve the measures used in protecting Personal Data so long as it does not diminish the level of data protection.

3.3 Security Breach Notification.

Docker shall notify Customer without undue delay but in no event later than seventy-two (72) hours of its discovery of a Security Breach.

3.4 Cooperation.

At Customer's request, Docker will reasonably support Customer or any Data Controller in dealing with requests from Data Subjects or regulatory authorities regarding Docker's processing of Personal Data.

3.5 Return or Deletion of Personal Data

Upon termination of the Agreement for whatever reason, and upon Customer's written request made within thirty (30) days after such termination, Docker will (as applicable) return to Customer or destroy all Personal Data. After such 30-day period, Docker will destroy such Personal Data.

4. SUBPROCESSORS

4.1 Permitted Use.

(a) Customer and Data Controllers authorize Docker to subcontract the processing of Personal Data to Subprocessors. Docker is responsible for any breaches of the Agreement caused by its Subprocessors.

(b) Subprocessors will have the same obligations in relation to Docker as Docker does as a Data Processor (or Subprocessor) with regard to their processing of Personal Data.

(c) Docker will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection. Subprocessors may have security certifications that evidence their use of appropriate security measures. If not, Docker will regularly evaluate each Subprocessor's security practices as they relate to data handling.

4.2 New Subprocessors.

Docker's use of Subprocessors is at its discretion, provided that:

(a) Docker will notify Customer in advance (by email or such other means which Docker makes available to its customers) of any changes to the list of Subprocessors in place on the Effective Date (except for Emergency Replacements or deletions of Subprocessors without replacement).

(b) If Customer has a legitimate reason that relates to the Subprocessors' processing of Personal Data, Customer may object to Docker's use of a Subprocessor, by notifying Docker in writing within thirty days after receipt of Docker's notice. If Customer objects to the use of the Subprocessor, the parties will come together in good faith to discuss a resolution. Docker may choose to: (i) not use the Subprocessor or (ii) take the corrective steps requested by Customer in its objection and use the Subprocessor. If none of these options are reasonably possible and Customer continues to object for a legitimate reason, either party may terminate the Agreement on thirty days' written notice. If Customer does not object within thirty days of receipt of the notice, Customer is deemed to have accepted the new Subprocessor.

(c) If Customer's objection remains unresolved sixty days after it was raised, and Docker has not received any notice of termination, Customer is deemed to accept the Subprocessor.

(d) The list of Subprocessors current as of the Effective Date shall be set forth in Appendix 1.

4.3 Emergency Replacement.

Docker may change a Subprocessor where the reason for the change is outside of Docker's reasonable control. In this case, Docker will inform Customer of the replacement Subprocessor as soon as possible. Customer retains its right to object to a replacement Subprocessor under Section 4.2(b).

5. INTERNATIONAL TRANSFERS

5.1 Limitations on International Transfer.

Personal Data from EEA, UK, or Swiss Data Controller(s) may only be exported to or accessed by Docker or its Subprocessors outside the EEA, the UK, or Switzerland, as applicable (**"International Transfer"**):

(a) If the recipient, or the country or territory in which it processes or accesses Personal Data, ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data as determined by the European Commission or another regulatory body of competent jurisdiction; or

(b) in accordance with Section 5.2.

5.2 Standard Contractual Clauses and Multi-tier Framework.

(a) The Standard Contractual Clauses apply where

(i) there is an International Transfer to a country that does not ensure an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data as determined by the European Commission or another regulatory body of competent jurisdiction, and/or

(ii) there is an International Transfer to a recipient that is not covered by an appropriate safeguard, including, but not limited to, binding corporate rules, an approved industry code of conduct, and individual adequacy decision by a regulatory body of competent jurisdictions, or an individual transfer authorisation granted by a regulatory body of competent jurisdiction.

(b) For Third Country Subprocessors, Docker shall ensure that such Subprocessor has entered into the unchanged version of the Standard Contractual Clauses prior to the Subprocessor's processing of Personal Data.

(c) Nothing in this DPA will be construed to prevail over any conflicting clause of the Standard Contractual Clauses.

6. DEFINITIONS

6.1 "Data Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

6.2 "Data Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

6.3 "Data Protection Law" means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement.

6.4 "Data Subject" means an identified or identifiable natural person.

6.5 "EEA" means the European Economic Area, namely the European Union Member States along with Iceland, Lichtenstein and Norway.

6.5a **"EU Standard Contractual Clauses"** shall mean the standard contractual clauses promulgated by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (C/2021/3972) on standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR.

6.6 "Personal Data" means any information relating to a Data Subject. For the purposes of this DPA, it includes only personal data entered into by or on behalf of Customer or its authorized users of the Service or derived from their use of the Service. It also includes personal data supplied to or accessed by Docker or its Subprocessors in order to provide support under the Agreement. Personal Data is a subset of Customer Data.

6.7 "Security Breach" means a confirmed accidental or unlawful destruction, loss, alteration, or disclosure that results in the compromise of the integrity and/or confidentiality of Personal Data. They include Appendices 1 and 2 attached to this DPA.

6.8 "Subprocessor" means Docker Affiliates and third parties engaged by Docker or Docker's Affiliates to process Personal Data.

6.9 "Territory" means the geography where Docker hosts Personal Data in the Service which is the United States.

6.10 "Third Country Subprocessor" means any Subprocessor incorporated outside the EEA and outside any country for which the European Commission has published an adequacy decision as published at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

6.11 "UK Standard Contractual Clauses" means either: (i) UK Data Transfer Addendum: the applicable EU Standard Contractual Clauses as amended by a data transfer addendum in a form adopted by the UK ICO, as amended, superseded or replaced from time to time; or (ii) UK Controller-Processor SCC: a data transfer agreement in the form published by the UK Information Commissioner's Office between a Controller as "data exporter" and a Processor as "data importer", as amended, superseded or replaced from time to time; or (iii) UK Controller-Controller Standard Contractual Clauses: a data transfer agreement in the form published by the UK Information Commissioner's Office between a Controller as "data exporter" and a Controller as "data importer", as amended, superseded or replaced from time to time.

7. LEGAL EFFECT

This DPA only becomes legally binding between Customer and Docker when Addendum has been fully executed or expressly incorporated within an Agreement that is fully executed. If this document has been electronically signed by either party, such signature will at least conform to the standard of an electronic signature as defined in art. 3 no. 10 of Regulation (EU) 910/2014 (eIDAS), and such signature will have the same legal affect as a hand written signature.

Appendix List

Appendix 1 – Details of Data Processing
Appendix 2 – Technical and Organizational Measures

Appendix 1
Details of Data Processing

Data Exporter

Name: The Customer or other Data Controller subscribed to a Service that allows authorized users to enter, amend, use, delete or otherwise process Personal Data, as identified in the Agreement.

Address: As stated in the Agreement.

Contact person's name, position and contact details: As stated in the Agreement.

Representative in the EU/UK, as applicable: not applicable

Role: (Controller/Processor): Controller

Data Importer
Name: Docker and its Subprocessors, each as identified in the Agreement.

Address: As stated in the Agreement.

Contact person's name, position and contact details: As stated in the Agreement.

Data protection officer: Wolfgang Steger. Privacy inquiries should be directed to privacy@docker.com.

Representative in the EU/UK, as applicable: Wolfgang Steger. Privacy inquiries should be directed to privacy@docker.com.

Role: (Controller/Processor): Processor

Purpose(s) of the data transfer and further processing

Provision by Docker of the Service that includes the following support:

- Monitoring the Service
- Release and development of fixes and upgrades to the Service
- Monitoring, troubleshooting and administering the underlying Service infrastructure
- Security monitoring, network-based intrusion detection support, penetration testing

Docker Affiliates provide support when a Customer submits a support ticket because the Service is not available or not working as expected for some or all authorized users. Docker answers phones and performs basic troubleshooting, and handles support tickets in a tracking system that is separate from the technical instance of the Service.

Description of Transfer

Categories of Data Subjects whose personal data is transferred
Unless provided otherwise by the Data Exporter, transferred Personal Data relates to the following categories of data subjects: employees, contractors, business partners or other individuals having been granted access credentials to the Service.
Categories of personal data transferred
The transferred Personal Data submitted into the Service may concern the following categories of data: Customer, in its sole discretion and control, determines the categories of Personal Data in accordance with the Service component(s) ordered under the Agreement. Customer can configure the data fields during implementation of the Service or as otherwise provided by the Service, subject

to the functionality of the related Service component(s). The transferred Personal Data submitted into the Service may include, but is not limited to the following categories of data:

- Data subject profile data (data subject name, contact information)
- Connection data

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
None.

Processing Operations (Activities relevant to the data transferred under the DPA)
The transferred Personal Data is subject to the following basic processing activities:

- use of Personal Data to set up, operate, monitor and provide the Service (including Operational and Technical Support)
- communication to authorized users
- upload any fixes or upgrades to the Service
- execution of instructions of Customer in accordance with the Agreement

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Continuous.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: As defined in the Agreement.

Competent supervisory authority: Netherlands.

Adequacy decisions and/or appropriate safeguards
The following adequacy decisions and/or appropriate safefguards will apply to this Processing: Not applicable.

List of Subcontractors as of the Effective Date

Company	Purpose	Hosting location
Amazon Web Services, Inc.	Cloud service provider	United States
Zendesk, Inc.	Cloud-based Customer support services	United States
Billforward	Cloud-based billing application	United States
Auth0	Single Sign-on provider	United States

Appendix 2
Technical and Organizational Measures

The following sections define the Docker's current technical and organizational security measures. Docker may change these at any time without notice so long as it maintains a comparable or better level of security. This may mean that individual measures are replaced by new measures that serve the same purpose without diminishing the security level.

Control		Data Importer's response:
Physical access control	Description of measures to prevent unauthorised third parties from accessing data processing systems (DP systems) that allow the processing or use of personal data.	Facilities containing systems are physically protected by key-card access, with access granted only to necessary personnel. Actual access to systems are controlled by multi-factor authentication.
Access control	Description of measures to prevent unauthorised third parties from using data processing systems that allow the processing or use of personal data.	Systems containing personal data are protected by userid and passwords requiring multi-factor authentication.
User access control	Description of measures to prevent persons from accessing data that is not considered mandatory in order to fulfil their tasks.	Access to systems are granted on a need-to-know basis in accordance with Data Importer's access policies. Access to systems is also promptly terminated in accordance with such polices.
Transmission control	Description of measures to prevent unauthorised third parties from accessing personal data during transmission and/or	Personal data is only transmitted electronically and over secured internet or network protocol.
Entry control	Description of measures to ensure consistent tracking if personal data has been entered, amended or removed from data processing systems and by	Information transmitted through systems are logged, tracked, and cross-referenced with account of Data Exporter.
Order control	Description of measures to ensure that personal data can only be processed in accordance with the instructions issued by the client.	Data Importer is contractually bound to use any personal data only in accordance with the terms of the Agreement between Data Importer and Data Exporter.
Availability control	Description of measures to protect personal data against accidental destruction or loss.	Not applicable. Data Importer is not a system of record.
Separation rule	Description of measures to ensure separate processing of different	Information transmitted through systems are logged, tracked, and cross-referenced with account of Data Exporter.

Appendix 3

STANDARD CONTRACTUAL CLAUSES

1. EU Standard Contractual Clauses

EU SCC term	Amendment / Selected option
Module	Module 2 (Controller to Processor)
Clause 7 (Docking clause)	not included
Clause 9 (Use of sub-processors) / Annex III	Option 2 shall apply. The list of sub-processors already authorised by Customers is contained in Appendix 1.
Clause 11 (Redress)	not included
Clause 13 (Supervision) and Annex 1.C	The supervisory authority with responsibility for ensuring compliance by the data exporter is: where the data exporter is established within an EU member state, the supervisory authority of that EU member state **OR** where the data exporter is subject to EU GDPR pursuant to Article 3(2) EU GDPR and has appointed a representative in [Note to supplier: where applicable, *insert country where representative is established*, the supervisory authority of that EU member state **OR** where the data exporter is subject to EU GDPR pursuant to Article 3(2) EU GDPR, but has not appointed a representative in an EU member state, the supervisory authority of the EU member state where the relevant data subjects are located.
Clause 17 (Governing law)	Laws of the Netherlands
Clause 18 (Choice of forum and jurisdiction)	Courts of the Netherlands
Annex I.A (List of parties)	The relevant data exporters and data importers are specified in Appendix 1.
Annex I.B (Description of the transfer)	The categories of data subject, personal data categories, purposes of international transfer and processing, any additional safeguards, and if applicable the duration of processing and any maximum data retention periods are specified in Appendix 1.

Annex II (Technical and organisational measures)	The relevant technical and organisational measures are specified in Appendix 2.

2. UK Standard Contractual Clauses

2.1 UK Data Transfer Addendum

UK Data Transfer Addendum *Incorporating EU Standard Contractual Clause terms*	**Amendment / Selected Option**
Clause 7 (Docking clause)	not included
Clause 9 (Use of sub-processors) / Annex III	Option 2 shall apply. The list of sub-processors already authorised by Customer is contained in Appendix 1.
Clause 11 (Redress)	not included
Clause 13 (Supervision) and Annex 1.C:	The competent supervisory authority is the UK Information Commissioner's Office.
Clause 17 (Governing law):	Laws of England
Clause 18 (Choice of forum and jurisdiction):	Courts of England and Wales
Clause 9	Clause 9 shall be amended to read: "The Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established, namely England".
Annex I.A (List of parties)	The relevant data exporters and data importers are specified in Appendix 1.
Annex I.B (Description of the transfer)	The categories of data subject, personal data categories, purposes of international transfer and processing, any additional safeguards, and if applicable the duration of processing and any maximum data retention periods are specified in Appendix 1.
Annex II (Technical and organisational measures)	The relevant technical and organisational measures are specified in Appendix 2.

2.2 UK Controller-Processor Standard Contractual Clauses

UK Controller-Processor SCC (2010/87/EU)_	**Amendment / Selected Option**
Appendix 1	Appendix 1 identifies: 1.1 the "data exporter(s)"; 1.2 the "data importers(s)"; 1.3 the categories of data subject whose personal data is transferred;

	1.4 the categories of Personal Data transferred (including special category data); 1.5 the activities of each of the "data importer(s)" and "data exporter(s)" and the purposes for which each uses the personal data being transferred; 1.6 the processing operations to which the Customer Personal Data transferred will be subject
Appendix 2	Appendix 2 identifies the relevant technical and organisational measures.
Clause 9 (Governing law)	Clause 9 shall be amended to read: "The Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established, namely England".