DOCKER DATA PROCESSING AGREEMENT

Last updated October 31, 2023

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 contacts regarding this DPA must be made to: privacy@docker.com.

1. DEFINITIONS

Capitalized terms shall have the meaning set out below. Any capitalized terms not defined in this DPA shall have the meaning set out in the Agreement or as otherwise defined in the applicable data protection laws and regulations:

"**Breach Event**": a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Personal Data transmitted, stored, or otherwise processed by Docker.

"**CCPA**" refers to the California Consumer Privacy Act of 2018 and its implementing regulations, as well as the California Privacy Rights Act of 2020.

"**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.

"**Customer**" means the entity using the Docker Services that has executed an Agreement, which references this DPA.

"**Processing**": any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Personal Data**": any information relating to an identified or identifiable natural person ("**Data Subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, which may be supplied to and Processed by Processor on behalf of the Controller pursuant to or in connection with the Agreement.

"**Processor**": Docker as the legal person who processes the Personal Data on behalf of the Customer.

"**Standard Contractual Clauses**": (i) the Standard Contractual Clauses approved by the Commission Decision 2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC ("**GDPR**") and (ii) the International Data Transfer Agreement issued by the Information Commissioner's Office in the United Kingdom ("**UK SCCs**").

"**Sub-Processor**": an entity engaged by the Processor exclusively for the Processing activities to be carried out pursuant to or in connection with the Agreement on behalf of the Controller and in accordance with its instructions, as transmitted by the Controller.

2. DURATION AND APPLICABLE LAWS

2.1. Unless otherwise agreed in writing, this DPA will take effect on the date of the Agreement's effective date and, notwithstanding its expiry, remain in effect until, and automatically expire upon, deletion of all Personal Data by Docker as described in this DPA.

2.2. This DPA applies when Personal Data is Processed by Docker as part of the provision of the Service, as further specified in the Agreement and the applicable order form, quote or equivalent

document.

2.3. The parties acknowledge and agree that the European data protection legislation, such as GDPR will apply to the processing of Controller Personal Data if, for example: i) the processing is carried out in the context of the activities of an establishment of Controller in the territory of the EEA; and/or ii) the Controller provides data that is personal data relating to Data Subjects who are in the EEA and the processing relates to the offering to them of goods or services in the EEA or the monitoring of their behavior in the EEA.

2.4. The Parties acknowledge and agree that non-European data protection legislation, such as the CCPA or the Brazilian Lei Geral de Proteção de Dados, may also apply to the processing of Controller Data.

2.5. The terms of this DPA will apply irrespective of whether the European data protection legislation or non-European data protection legislation applies to the processing of Controller data.

3. DATA PROCESSING

3.1. To the extent that the GDPR or other privacy Laws and regulations with analogous terms apply to Docker's Processing of Personal Data on behalf of the Customer under the Agreement, Docker is the Processor to the Customer, who can act either as the controller or processor of Personal Data, as those or analogous terms are defined under applicable legislation.

3.2. To the extent that the CCPA applies to Docker Processing of Personal Data on behalf of Customer under the Agreement, (a) Customer is the "Business" and Docker is the "Service Provider"; (b) Docker will Process Personal Data solely on behalf of Customer and for the specific business purposes set forth in the Agreement; and (c) Docker will not retain, use, disclose, or otherwise Process such Personal Data for any purpose other than for the specific purpose of performing the Service as specified in the Agreement.

3.3. Docker will process the Personal Data in accordance with the Customer's instructions and applicable laws: (a) to provide the Service, (b) as documented in the Agreement, including this DPA; and (c) as further documented in any other written instructions given by Customer and acknowledged by Docker as constituting instructions for purposes of this DPA. Docker will comply with all lawful and reasonable Controller instructions. If Docker cannot comply with an instruction, it will notify the Customer without undue delay.

3.4. The nature and purpose of the Processing and the type of Personal Data and categories of Data Subjects about whom Personal Data shall be processed are determined by Customer, based on Customer's use of the Services and the Personal Data that Customer chooses to upload to the Service(s) or otherwise provide to Docker for the purpose of Processing. The categories of Data Subjects may include Customer's employees, staff, vendors, end users, or the Personal Data of any other Individuals whom Customer chooses to provide to Docker under the Agreement. Details of the data processing are further described in Appendix 1.

3.5. At Customer's request, Docker will reasonably support the Customer or any Data Controller in dealing with requests from Data Subjects or regulatory authorities regarding Docker's processing of Personal Data under this DPA. Where requested to do so by the Customer, Docker shall disclose the information reasonably required to demonstrate compliance with the applicable data protection Laws, including the necessary information for the Customer to carry out a privacy impact assessment of the Services and implement mitigation actions agreed by the Parties to address privacy risks which may have been identified.

3.6. Docker shall, upon request, make available to the Controller information reasonably necessary to demonstrate compliance with this DPA and/or the necessary information for the Controller to carry out a privacy impact assessment of the Service and in implementing mitigation actions agreed by the Parties to address privacy risks which may have been identified.

3.7. 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. DATA SECURITY

4.1. Docker will implement and maintain technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access ("Security Measures"). Those are further described in Appendix 2. Docker may update or modify the Security Measures from time to time at its discretion, provided that such updates and modifications do not result in the degradation of the overall security of the Service.

4.2. Docker will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors, and Sub-processors to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Docker maintains a list of Sub-processors available for consultation at https://www.docker.com/trust/privacy/sub-processors/

4.3. Docker is regularly audited by independent third parties and holds a SOC 2 Type I attestation report.

4.4.Docker will assist Customer in ensuring compliance with any of its obligations in respect of security of Personal Data and Breach Events.

4.5. Docker shall notify Customer without undue delay but in no event later than seventy-two (72) hours after becoming aware of any Breach Event.

5. SUB-PROCESSORS

5.1. Customer acknowledges and agrees that may engage Sub-Processor(s) in the performance of the Service(s) on Customer's behalf. All Sub-Processors to whom Docker transfers Personal Data are bound by substantially the same material obligations as Docker undertakes under this DPA and provide adequate guarantees of security and compliance. Docker will be liable for the acts and omissions of its Sub-Processors to the same extent that Docker would be liable if performing the Service directly, under the terms of the Agreement.

5.2. The current Sub-Processors are listed as per Section 4.2 above. Docker may use new Sub-Processors provided it notifies the Customer in advance of any changes to the list of Sub-Processors in place on the effective date. If Customer has a legitimate reason, Customer may object to Docker's use of a Sub-Processor, by notifying Docker in writing within thirty days after receipt of Docker's notice. If the Customer objects to the use of the Sub-Processor, the parties will come together in good faith to discuss a resolution. Docker may choose to: (i) not use the Sub-Processor or (ii) take the corrective steps requested by Customer in its objection and use the Sub-Processor. If none of these options is 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 Sub-Processor.

6. INTERNATIONAL TRANSFERS

6.1. Docker is self-certified pursuant to the EU-US Data Privacy Framework. Customer may elect to rely on that adequacy decision to allow international transfers or choose to enter into the applicable Standard Contractual Clauses mentioned in Appendix 1.

6.2. Where (i) Customer transfers Personal Data within the European Economic Area, the United Kingdom, or Switzerland to Docker (where such transfer includes Personal Data subject to the GDPR), and (ii) Docker will be Processing such Personal Data in a country that (a) is not subject to an

adequacy decision of the EU Commission (or in case such adequacy decision is invalidated) and (b) does not provide an adequate level of protection within the meaning of applicable Privacy Laws and Regulations, the Parties shall enter into the appropriate Standard Contractual Clauses mentioned in Appendix 1. Nothing in this DPA will be construed to prevail over any conflicting clause of the Standard Contractual Clauses.

7. DISCLOSURE TO COMPETENT AUTHORITIES

7.1 Docker may disclose Personal Data if required by law or a subpoena or other judicial or administrative order or if Docker deems the disclosure necessary to protect the safety and rights of any person, or the general public.

7.2 Docker undertakes to adopt supplementary measures to protect the Personal Data transferred under the SCCs in accordance with the requirements of applicable privacy laws, including by implementing appropriate technical and organizational safeguards, such as encryption or similar technologies, access controls or other compensating controls, to protect SCC personal data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defense and public security.

7.3 In the event that Docker receives a legally binding request for access to the Personal Data by a public authority, Docker will:

7.3.1. promptly notify Customer of such request to enable Customer to intervene and seek relief from such disclosure, unless Docker is otherwise prohibited from providing such notice. If Docker is so prohibited: i) It will use its reasonable efforts to obtain the right to waive this prohibition, to communicate as much information as it can, and be able to demonstrate that it did so; ii) In the event that, despite having used its reasonable efforts, Docker is not permitted to notify Customer, it will make available general information, on an annual basis, and as allowed by law (such as a transfer impact assessment or other transparency report), concerning the requests it received to the Customer and/or the competent supervisory authority of the Customer.

7.3.2. not make any disclosures of the Personal Data, to any public authority, that are determined to be massive, disproportionate, and indiscriminate in a manner that it would go beyond what is necessary in a democratic society; and

7.3.3 upon request from the Customer, provide general information on the requests from public authorities it received in the preceding twelve (12) month period relating to the Personal Data.

8. APPLICABLE LAW AND JURISDICTION

This DPA shall be governed by, and construed and enforced in accordance with, the governing clause established in the Agreement. In the absence of a governing clause, the law of Docker's registered office shall apply.

Appendix List

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

Appendix 1

A - Subject Matter and Details of the Data Processing

Subject Matter
Docker's provision of the Services and related technical support to Customer.

Duration of the Processing
The applicable term plus the period from expiry of such term until deletion of all Controller Data by Customer in accordance with the Data Processing Agreement.

Nature and Purpose of the Processing
Customer will process Controller Personal Data submitted, stored, sent or received by Customer, its Affiliates or end users via the Services for the purposes of monitoring and providing the Services and related technical support to Controller in accordance with the Data Processing Agreement.

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.

Categories of Data
Personal data submitted, stored, sent or received by Customer, its Affiliates or end users via the Services may include employees, contractors, business partners or other individuals having been granted access credentials to the Service. 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 the implementation of the Service or as otherwise provided by the Service, subject to the functionality of the related Service component(s).

The Personal Data submitted into the Service may include, but is not limited to the following categories of data: i) Data Subject profile data (data subject name, contact information) and ii) connection data.

Frequency of the transfer: 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.

List of Sub-Processors and Locations

A list of Docker's current Sub-Processors, including a description of their processing activities and locations, is made available on Docker's webpage accessible at https://www.docker.com/trust/privacy/sub-processors/

.

B – International Transfers

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 Sub-Processors, 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

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

In case the controller is an EU entity the Parties shall enter into the model of SCC Clauses (standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council) found at https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en

In case the controller is an UK entity, the Parties shall enter into the international data transfer agreement (IDTA), found at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/

Appendix 2
Technical and Organizational Measures

The following sections define 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.

Encryption	Docker has and will maintain: (i) an established method to encrypt Customer Data in transit and at rest; (ii) an established method to securely store passwords following industry standard practices; and (iii) use established key management methods. Customer Data is encrypted in transit over public networks using TLS 1.2 or greater, with Perfect Forward Secrecy (PFS) to protect it from unauthorized disclosure or modification. Data stored on cloud hosting providers holding Customer Data industry-standard, AES256 encryption at rest.
Pseudonymisation	Docker has and will maintain: (i) an established method to create pseudonymised data sets using industry standard practices; and (ii) appropriate technical and organizational measures governing the systems capable of remapping pseudonymous identifiers.
Access control	Systems containing personal data are protected by user ID and passwords requiring multi-factor authentication.
User access control	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 policies.
Transmission control	Personal data is only transmitted electronically and over secured internet or network protocol.
Entry control	Information transmitted through systems are logged, tracked, and cross-referenced with the Customer account.
Order control	Docker is contractually bound to use any personal data only in accordance with the terms of the Agreement between Docker and Customer.
Availability control	Not applicable. Docker is not a system of record.
Separation rule	Information transmitted through systems are logged, tracked, and cross-referenced with the Customer account.