



# Data Processing Agreement

Last Updated on November 30, 2021

## 1. Scope, Order of Precedence, and Term

**1.1** This Data Processing Agreement (“**DPA**”) is an addendum to the Customer Terms of Service (“**Agreement**”) between DigitalOcean, LLC (“**DigitalOcean**”) and the Customer. DigitalOcean and Customer are individually a “**party**” and, collectively, the “**parties**.”

**1.2** This DPA applies where and only to the extent that DigitalOcean processes Personal Data on behalf of the Customer in the course of providing the Services and such Personal Data is subject to Data Protection Laws of the appropriate jurisdiction, including the State of California, the European Union, the European Economic Area and/or its member states, Switzerland and/or the United Kingdom. The parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.

**1.3** The duration of the Processing covered by this DPA shall be in accordance with the duration of the Agreement.



## 2. Definitions

**2.1** The following terms have the meanings set forth below. All capitalized terms not defined in this DPA will have the meanings set forth in the Agreement.

**2.2** The following terms have the definitions given to them in the CCPA: “**Business**,” “**Sell**,” “**Service Provider**,” and “**Third Party**.”

**2.3 “Controller”** means the entity that determines the purposes and means of the Processing of Personal Data. “Controller” includes equivalent terms in other Data Protection Law, such as the CCPA-defined term “**Business**” or “**Third Party**,” as context requires.

**2.4 “Data Protection Law”** means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement as it relates to the Customer, including Regulation 2016/679 (General Data Protection Regulation) (“**GDPR**”), and Cal. Civ. Code Title 1.81.5, § 1798.100 et seq. (California Consumer Privacy Act) (“**CCPA**”).

**2.5 “Data Subject”** means an identified or identifiable natural person.

**2.6 “De-identified Data”** means a data set that does not contain any Personal Data. Aggregated data is De-identified Data. To “**De-identify**” means to create De-identified Data from Personal Data.

**2.7 “EEA”** means the European Economic Area.

**2.8 “Standard Contractual Clauses”** means the European Union standard contractual clauses for international transfers from the European Economic Area



to third countries, Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

**2.9 “Personal Data”** means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a Data Subject in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. “Personal Data” includes equivalent terms in other Data Protection Law, such as the CCPA-defined term “Personal Information,” as context requires.

**2.10 “Personal Data Breach”** means a breach of security of the Services leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

**2.11 “Process” or “Processing”** means any operation or set of operations which is performed upon Personal Data, whether by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

**2.12 “Processor”** means an entity that processes Personal Data on behalf of another entity. “Processor” includes equivalent terms in other Data Protection Law, such as the CCPA-defined term “Service Provider,” as context requires.

**2.13 “Sensitive Data”** means the following types and categories of data: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs,



or trade union membership; genetic data; biometric data; data concerning health, including protected health information governed by the Health Insurance Portability and Accountability Act; data concerning a natural person's sex life or sexual orientation; government identification numbers (e.g., SSNs, driver's license); payment card information; nonpublic personal information governed by the Gramm Leach Bliley Act; an unencrypted identifier in combination with a password or other access code that would permit access to a data subject's account; and precise geolocation.

**2.14 "Subprocessor"** means a Processor engaged by a party who is acting as a Processor.

### **3. Description of the Parties' Personal Data Processing Activities and Statuses of the Parties**

**3.1** Schedules 1-3 attached hereto describe the purposes of the parties' Processing, the types or categories of Personal Data involved in the Processing, and the categories of Data Subjects affected by the Processing.

**3.2** Schedules 1-3 list the parties' statuses under relevant Data Protection Law.

### **4. International Data Transfer**

**4.1** With respect to Personal Data of Data Subjects located in the EEA, Switzerland, or the United Kingdom that Customer transfers to DigitalOcean or permits DigitalOcean to access, the parties agree that by executing this DPA they also execute the Standard Contractual Clauses, which will be incorporated by



reference and form an integral part of this DPA. The parties agree that, with respect to the elements of the Standard Contractual Clauses that require the parties' input, Schedules 1-3 contain all the relevant information.

## 5. Data Protection Generally

**5.1 Compliance.** The parties will comply with their respective obligations under Data Protection Law and their privacy notices.

**5.2 Customer Processing of Personal Data.** Customer represents and warrants that it has the consent or other lawful basis necessary to collect Personal Data in connection with the Services.

**5.3 Cooperation.**

**5.3.1 Data Subject Requests.** The parties will provide each other with reasonable assistance to enable each to comply with their obligations to respond to Data Subjects' requests to exercise rights that those Data Subjects may be entitled to under Data Protection Law.

**5.3.2 Governmental and Investigatory Requests.** Customer will promptly notify DigitalOcean if Customer receives a complaint or inquiry from a regulatory authority indicating that DigitalOcean has or is violating Data Protection Law.

**5.3.3 Other Requirements of Data Protection Law.** Upon request, the parties will provide relevant information to each other to fulfill their respective



obligations (if any) to conduct data protection impact assessments or prior consultations with data protection authorities.

**5.4 Confidentiality.** The parties will ensure that their employees, independent contractors, agents, and representatives are subject to an obligation to keep Personal Data confidential and have received training on data privacy and security that is commensurate with their responsibilities and the nature of the Personal Data.

**5.5 De-identified, Anonymized, or Aggregated Data.** The parties may create De-identified Data from Personal Data and Process the De-identified Data for any purpose.

## **6. Data Security**

**6.1 Security Controls.** Each party will maintain written information security policy that defines security controls that are based on the party's assessment of risk to Personal Data that the party Processes and the party's information systems. DigitalOcean's security controls are described in Schedule 2.3 and Schedule 3.4.

## **7. DigitalOcean's Obligations as a Processor, Subprocessor, or Service Provider**

**7.1** DigitalOcean will have the obligations set forth in this Section 7 if it Processes Personal Data in its capacity as Customer's Processor or Service Provider; for



clarity, these obligations do not apply to DigitalOcean in its capacity as a Controller, Business, or Third party.

## **7.2** Scope of Processing.

**7.2.1** DigitalOcean will Process Personal Data to provide Services to Customer under the Agreement, and comply with applicable law. DigitalOcean will notify Customer if the law changes and those changes cause DigitalOcean not to be able to comply with the Agreement.

**7.3** Data Subjects' Requests to Exercise Rights. DigitalOcean will promptly inform Customer if DigitalOcean receives a request from a Data Subject to exercise their rights with respect to their Personal Data under applicable Data Protection Law. Customer will be responsible for responding to such requests. DigitalOcean will not respond to such Data Subjects except to acknowledge their requests. DigitalOcean will provide Customer with commercially reasonable assistance, upon request, to help Customer to respond to a Data Subject's request.

## **7.4** DigitalOcean's Subprocessors.

**7.4.1** Existing Subprocessors. Customer agrees that DigitalOcean may use the Subprocessors listed at Schedule 3.

**7.4.2** Use of Subprocessors. Customer grants DigitalOcean general authorization to engage Subprocessors if DigitalOcean and a Subprocessor enter into an agreement that requires the Subprocessor to meet obligations that are no less protective than this DPA.



**7.4.3** Notification of Additions or Changes to Subprocessors. DigitalOcean will notify Customer of any additions to or replacements of its Subprocessors via email or other contact methods and make that list available on Customer's request. DigitalOcean will provide Customer with at least 30 days to object to the addition or replacement of Subprocessors in connection with DigitalOcean's performance under the Agreement, calculated from the date DigitalOcean provides notice to Customer. If Customer reasonably objects to the addition or replacement of DigitalOcean's Subprocessor, DigitalOcean will immediately cease using that Subprocessor in connection with DigitalOcean's Services under the Agreement, and the parties will enter into good faith negotiations to resolve the matter. If the parties are unable to resolve the matter within 15 days of Customer's reasonable objection (which deadline the parties may extend by written agreement), Customer may terminate the Agreement and/or any statement of work, purchase order, or other written agreements. The parties agree that DigitalOcean has sole discretion to determine whether Customer's objection is reasonable; however, the parties agree that Customer's objection is presumptively reasonable if the Subprocessor is a competitor of Customer and Customer has a reason to believe that competitor could obtain a competitive advantage from the Personal Data DigitalOcean discloses to it, or Customer anticipates that DigitalOcean's use of the Subprocessor would be contrary to law applicable to Customer.

**7.4.4** Liability for Subprocessors. DigitalOcean will be liable for the acts or omissions of its Subprocessors to the same extent as DigitalOcean would



be liable if performing the services of the Subprocessor directly under the DPA, except as otherwise set forth in the Agreement.

**7.5 Personal Data Breach.** DigitalOcean will notify Customer without undue delay of a Personal Data Breach affecting Personal Data DigitalOcean Processes in connection with the Services. Upon request, DigitalOcean will provide information to Customer about the Personal Data Breach to the extent necessary for Customer to fulfill any obligations it has to investigate or notify authorities, except that DigitalOcean reserves the right to redact information that is confidential or competitively sensitive. Notifications will be delivered to the email address Customer provides in Customer's account. Customer agrees that email notification of a Personal Data Breach is sufficient. DigitalOcean agrees that it will notify Customer if it changes its contact information. Customer agrees that DigitalOcean may not notify Customer of security-related events that do not result in a Personal Data Breach.

**7.6 Deletion and Return of Personal Data.** Upon deactivation of the Services, all Personal Data shall be deleted, save that this requirement shall not apply to the extent DigitalOcean is required by applicable law to retain some or all of the Personal Data, or to Personal Data it has archived on back-up systems, which such Personal Data DigitalOcean shall securely isolate and protect from any further processing, except to the extent required by applicable law.

**7.7 Audits.**

**7.7.1** DigitalOcean shall maintain records of its security standards. Upon Customer's written request, DigitalOcean shall provide (on a confidential



basis) copies of relevant external ISMS certifications, audit report summaries and/or other documentation reasonably required by Customer to verify DigitalOcean's compliance with this DPA. DigitalOcean shall further provide written responses (on a confidential basis) to all reasonable requests for information made by Customer, including responses to information security and audit questionnaires, that Customer (acting reasonably) considers necessary to confirm DigitalOcean's compliance with this DPA, provided that Customer shall not exercise this right more than once per year.

**7.7.2** To the extent the Standard Contractual Clauses apply and the Customer reasonably argues and establishes that the above documentation and/or other third party audit reports are not sufficient to demonstrate compliance with the obligations laid down in this DPA, the Customer may execute an audit as outlined under Clause 8.9 of the Standard Contractual Clauses accordingly, provided that in such an event, the parties agree: (a) Customer is responsible for all costs and fees relating to such audit (including for time, cost and materials expended by DigitalOcean); (b) a third party auditor must be mutually agreed upon between the parties to follow industry standard and appropriate audit procedures; © such audit must not unreasonably interfere with DigitalOcean's business activities and must be reasonable in time and scope; and (d) the parties must agree to a specific audit plan prior to any such audit, which must be negotiated in good faith between the parties. For avoidance of doubt, nothing in this Section 7.7.2 modifies or varies the Standard Contractual Clauses, and to the extent a competent authority finds otherwise or any portion of Section



7.7.2 is otherwise prohibited, unenforceable or inappropriate in view of the Standard Contractual Clauses, the relevant portion shall be severed and the remaining provisions hereof shall not be affected.

## Schedule 1: Description of the Processing and Subprocessors

Processing Activity	Status of the Parties	Categories of Personal Data Processed	Categories of Sensitive Data Processed	Frequency of Transfer	Applicable SCCs Module
Customer discloses Personal Data to DigitalOcean to provide, operate, and maintain DigitalOcean Services.	Customer is a Controller.  DigitalOcean is a Controller.	Account registration, payment information, user content, communications, cookies and other tracking technologies, usage of Services, and third party accounts.	None	Continuous	Module 1



Customer discloses Personal Data to improve, analyze, personalize, and DigitalOcean Services.	Customer is a Controller.  DigitalOcean is a Controller.	Account registration, payment information, user content, communications, cookies and other tracking technologies, usage of Services, and third party accounts.	None	Continuous	Module 1
Customer contacts DigitalOcean for support.	Customer is a Controller.  DigitalOcean is a Controller.	Account registration, payment information, user content, communications, usage of Services, and third party accounts.	None	Continuous	Module 1
Customer stores end-user data on DigitalOcean Services.	DigitalOcean is a Processor.  Customer is a Controller or processor to a controller.	As determined by Customer.	As determined by Customer.	As determined by Customer.	Module 2  or Module 3 (if Customer is a processor to another controller)



## Schedule 2: Controller-to-Controller Information for International Data Transfers

### 1. Retention Periods

DigitalOcean retains Personal Data it collects as a Controller for as long as DigitalOcean has a business purpose for it or for the longest time allowable by applicable law.

### 2. Information for International Transfers

For the purposes of the Standard Contractual Clauses:

- Clause 11(a), Module 1: The parties do **not** select the independent dispute resolution option.
- Clause 17, Module 1: The parties select Option 1. The Member State is: Netherlands.
- Clause 18(b), Module 1: The Parties agree that those shall be the courts of Netherlands.
- Annex I(A): The data exporter is Customer. The data importer is DigitalOcean. Contact details for Customer is the email address(s) designated by Customer in Customer's DigitalOcean account. Contact detail for DigitalOcean is: [privacy@digitalocean.com](mailto:privacy@digitalocean.com).
- Annex I(B): The parties agree that Schedule 1 describes the transfer.
- Annex I©: The competent supervisory authority is the supervisory authority of: The Dutch Data protection Authority (Autoriteit Persoonsgegevens)
- Annex II: The parties agree that Schedule 2.3 describes the technical and organizational measures applicable to the transfer.



For definitions of these terms please review our [Privacy Policy \(Section 1\)](#)

### 3. Technical and Organizational Measures

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security Measure
Measures of pseudonymisation and encryption of personal data	DigitalOcean's databases that store Customer Personal Data are encrypted using the Advanced Encryption Standard (AES). Customer data is encrypted in transit between the Customer's software application and DigitalOcean using TLS v1.2.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services  Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	DigitalOcean uses a variety of tools and mechanisms to achieve high availability and resiliency. DigitalOcean's infrastructure spans multiple fault-independent availability zones in geographic regions physically separated from one another. DigitalOcean's infrastructure is able to detect and route around issues experienced by hosts or even whole data centers in real time and employ orchestration tooling that has the ability to regenerate hosts, building them from the latest backup. DigitalOcean also leverages specialized tools that monitor server performance, data, and traffic load capacity within each availability zone and colocation data center. If suboptimal server performance or overloaded capacity is detected on a server within an availability zone or colocation data center, these tools increase the capacity or shift traffic to relieve any suboptimal server performance or capacity overload. DigitalOcean is also immediately notified in the event of any suboptimal server performance or overloaded capacity.



Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	<p>DigitalOcean has developed and implemented a security control environment designed to protect the confidentiality, integrity, and availability of customers' systems. The Customer Data Use Policy governs the requirements for use of customer data in accordance with several industry standards.</p> <p>DigitalOcean conducts a variety of regular internal and external audits that are inclusive of security operations. For more information please visit: <a href="https://www.digitalocean.com/trust/certification-reports/">https://www.digitalocean.com/trust/certification-reports/</a></p>
Measures for user identification and authorization	<p>Access control policies require that access to DigitalOcean assets be granted based on business justification, with the asset owner's authorization and limits based on "need to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews. Documentation of these requirements is recorded and provided to external auditors for security certification testing.</p>
Measures for the protection of data during transmission  Measures for the protection of data during storage	<p>DigitalOcean's databases that store Customer Personal Data are encrypted using the Advanced Encryption Standard (AES). Customer data stored by DigitalOcean is encrypted in transit between the Customer's software application and DigitalOcean using TLS v1.2.</p>



Measures for ensuring physical security of locations at which personal data are processed	<p>DigitalOcean data centers are located in nondescript buildings that are physically constructed, managed, and monitored 24 hours a day to protect data and services from unauthorized access as well as environmental threats. All data centers are surrounded by a fence with access restricted through badge controlled gates.</p> <p>CCTV is used to monitor physical access to data centers and the information systems. Cameras are positioned to monitor perimeter doors, facility entrances and exits, interior aisles, caged areas, high-security areas, shipping and receiving, facility external areas such as parking lots and other areas of the facilities.</p>
Measures for ensuring events logging	<p>Logging of service, user and security events (web server logs, FTP server logs, etc.) is enabled and retained centrally. DigitalOcean restricts access to audit logs to authorized personnel based on job responsibilities.</p> <p>Audit logging procedures are reviewed as part of external audits for security standards.</p>
Measures for internal IT and IT security governance and management  Measures for certification/assurance of processes and products	<p>DigitalOcean has developed and implemented a security control environment designed to protect the confidentiality, integrity, and availability of customers' systems. DigitalOcean performs an annual internal review of all security management policies and procedures. External auditors perform an annual review of these policies and procedures.</p> <p>DigitalOcean conducts a variety of regular internal and external audits that are inclusive of security operations. For more information please visit: <a href="https://www.digitalocean.com/trust/certification-reports/">https://www.digitalocean.com/trust/certification-reports/</a>.</p>



Measures for ensuring data minimisation	More information about how DigitalOcean processes personal data is set forth in the Privacy Policy available at: <a href="https://www.digitalocean.com/legal/privacy-policy/">https://www.digitalocean.com/legal/privacy-policy/</a> .
Measures for ensuring data quality	
Measures for ensuring limited data retention	
Measures for ensuring accountability	
Measures for allowing data portability and ensuring erasure	



Technical and organizational measures to be taken by the [sub]-processor to provide assistance to the controller and, for transfers from a processor to a [sub]-processor, to the Customer.	When DigitalOcean engages a Subprocessor, DigitalOcean and the Subprocessor enter into an agreement with data protection obligations substantially similar to those contained in this Schedule. Each Subprocessor agreement must ensure that DigitalOcean is able to meet its obligations to Customer. In addition to implementing technical and organizational measures to protect personal data, sub-processors must (a) notify DigitalOcean in the event of a Security Incident so DigitalOcean may notify Customer; (b) delete personal data when instructed by DigitalOcean in accordance with Customer's instructions to DigitalOcean; © not engage additional sub-processors without DigitalOcean's authorization; (d) not change the location where personal data is processed; or (e) process personal data in a manner which conflicts with Customer's instructions to DigitalOcean.
---	--



## Schedule 3: Controller-to-Processor and/or Processor-to-Processor Information for International Data Transfers

### 1. Subprocessors

DigitalOcean uses Subprocessors when it acts as a Processor. Customer authorizes DigitalOcean to use these Subprocessors consistent with Section 7.4. Subprocessors are available upon request at [privacy@digitalocean.com](mailto:privacy@digitalocean.com).

### 2. Retention Periods

DigitalOcean retains Personal Data it collects or receives from Customer as a Processor for the duration of the Agreement and consistent with its obligations in this DPA.

### 3. Information for International Transfers

For the purposes of the Standard Contractual Clauses:

- Clause 9, Module 2(a): The parties select Option 2. The time period is 5 days.
- Clause 11(a): The parties do **not** select the independent dispute resolution option.
- Clause 17, Module 2: The parties select Option 2. The Member State of the data exporter is: EU Member State Customer is located in.
- Clause 18(b), Module 2: The Parties agree that those shall be the courts of the EU Member State Customer is located in.
- Annex I(A): The data exporter is Customer. The data importer is DigitalOcean. Contact details for Customer is the email address(s)



designated by Customer in Customer's DigitalOcean account. Contact detail for DigitalOcean is: [privacy@digitalocean.com](mailto:privacy@digitalocean.com).

- Annex I(B): The parties agree that Schedule 1 describes the transfer.
- Annex I©: The competent supervisory authority is the supervisory authority of: Customer who acts as data exporter.
- Annex II: The parties agree that Schedule 3.4 describes the technical and organizational measures applicable to the transfer.

#### 4. Technical and Organizational Measures

Technical and Organizational Security Measure	Evidence of Technical and Organizational Security Measure
Measures of pseudonymisation and encryption of personal data  Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Customer responsibility. Please see DigitalOcean's Trust Platform FAQ for more information on the Separation of Responsibilities: <a href="https://www.digitalocean.com/trust/faq/">https://www.digitalocean.com/trust/faq/</a> .
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of	Customer responsibility: It is the responsibility of the customer to backup and utilize redundancy mechanisms to protect their content data.



a physical or technical incident	
<p>Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing</p> <p>Measures for user identification and authorization</p> <p>Measures for the protection of data during transmission</p> <p>Measures for the protection of data during storage</p>	<p>Customer responsibility. Please see DigitalOcean's Trust Platform FAQ for more information on the Separation of Responsibilities: <a href="https://www.digitalocean.com/trust/faq/">https://www.digitalocean.com/trust/faq/</a>.</p>



Measures for ensuring physical security of locations at which personal data are processed	<p>DigitalOcean data centers are located in nondescript buildings that are physically constructed, managed, and monitored 24 hours a day to protect data and services from unauthorized access as well as environmental threats. All data centers are surrounded by a fence with access restricted through badge controlled gates.</p> <p>CCTV is used to monitor physical access to data centers and the information systems. Cameras are positioned to monitor perimeter doors, facility entrances and exits, interior aisles, caged areas, high-security areas, shipping and receiving, facility external areas such as parking lots and other areas of the facilities.</p>
<p>Measures for ensuring events logging</p> <p>Measures for internal IT and IT security governance and management</p> <p>Measures for certification/assurance of processes and products</p> <p>Measures for ensuring data minimisation</p> <p>Measures for ensuring data quality</p> <p>Measures for ensuring limited data retention</p>	<p>Customer responsibility. Please see DigitalOcean's Trust Platform FAQ for more information on the Separation of Responsibilities: <a href="https://www.digitalocean.com/trust/faq/">https://www.digitalocean.com/trust/faq/</a>.</p>



Measures for ensuring accountability	
Measures for allowing data portability and ensuring erasure	Customer is able to export or delete Customer Content using the self-service features of the Services as set forth in the applicable documentation for the Services available at <a href="https://www.digitalocean.com/trust/data-portability/">https://www.digitalocean.com/trust/data-portability/</a>
Technical and organizational measures to be taken by the [sub]-processor to provide assistance to the controller and, for transfers from a processor to a [sub]-processor, to the Customer.	Customer responsibility. Please see DigitalOcean's Trust Platform FAQ for more information on the Separation of Responsibilities: <a href="https://www.digitalocean.com/trust/faq/">https://www.digitalocean.com/trust/faq/</a> .

## Schedule 4: CCPA Addendum

[CCPA Data Processing Addendum](#)