DIGITALOCEAN, LLC

APEC PRIVACY RECOGNITION FOR PROCESSORS CERTIFICATION REPORT

FOR

CLOUD INFRASTRUCTURE PLATFORM

NOVEMBER 8, 2024

Assessment and Compliance Services

Statement of Confidentiality

The sole purpose of this document is to provide DigitalOcean, LLC ("DigitalOcean") with the results of the Asia-Pacific Economic Cooperation ("APEC") Privacy Recognition for Processors ("PRP") certification assessment. This document, and any other DigitalOcean related information provided, shall remain the sole property of DigitalOcean and may not be copied, reproduced, or distributed without the prior written consent of DigitalOcean.

Applicability

The information found in this Report and the conclusions reached were dependent upon the complete and accurate disclosure of information by DigitalOcean.

Independence Disclosure

Schellman Compliance, LLC ("Schellman") assessed the Cloud Infrastructure Platform for DigitalOcean. Schellman does not hold any investment or control over DigitalOcean. During the course of the assessment, Schellman did not willfully and unnecessarily market services to achieve conformance to APEC PRP. No Schellman service was recommended during the course of the engagement.

TABLE OF CONTENTS

SECTION 1 AUDIT TEAM RECOMMENDATION.....1
SECTION 2 EXECUTIVE SUMMARY 3
SECTION 3 TESTING RESULTS 10

SECTION 1

AUDIT TEAM RECOMMENDATION

AUDIT TEAM RECOMMENDATION

Summary of Findings and Recommendation

The client has met the requirements of the APEC PRP minimum certification requirements. There were no areas of noncompliance noted as a result of the 2024 certification assessment.

DigitalOcean is required to maintain compliance with the requirements throughout the next 12 months. DigitalOcean is required to contact Schellman if any of their policies or procedures change related to the Cloud Infrastructure Platform and the minimum certification requirements. Schellman will contact DigitalOcean if a valid complaint is filed related to the APEC PRP certification. Ongoing monitoring is required throughout the certification period, which may include periodic reviews of DigitalOcean's data processing agreement for updates or investigations into any disputes received by Schellman. Documentation may be requested by Schellman of DigitalOcean to validate compliance or onsite visits. Schellman will notify DigitalOcean in advance to allow for documentation collection and scheduling of the onsite visit.

SECTION 2

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

Introduction and Certification Scope

DigitalOcean, LLC ("DigitalOcean") contracted with Schellman Compliance, LLC to perform a certification assessment to determine conformance with the APEC PRP minimum certification requirements for the Cloud Infrastructure Platform.

The scope of the review was limited to DigitalOcean's Cloud Infrastructure Platform in the role of a processor processing personal data on behalf of their customers, the controllers.

Company Background

DigitalOcean, founded in 2012, provides cloud services to deploy, manage, and scale applications with the intent of removing infrastructure friction and providing predictability. The DigitalOcean cloud services provide its customers with a user interface and application programming interfaces ("APIs"), a robust set of features, tutorials, and a library of open source resources.

Description of Services Provided

DigitalOcean's Cloud Infrastructure Platform allows users to build, deploy, and scale applications while leveraging the services of DigitalOcean for the handling, provisioning, and managing of infrastructure, databases, and operating systems. Furthermore, DigitalOcean's products and services are virtualized to help ensure it has the ability to scale to meet demand.

DigitalOcean provides Infrastructure as a Service ("IaaS"), Platform as a Service ("PaaS"), and Function as a Service ("FaaS") offerings. The various products for each of DigitalOcean's IaaS, PaaS, and FaaS offerings are described below:

IaaS Offerings

Droplets

Droplets are Linux-based virtual machines ("VMs") that run on top of virtualized hardware. Each Droplet created is a new server customers can use, either standalone or as part of a larger, cloud-based infrastructure.

GPU Droplets

GPU Droplets are Linux-based VMs that run on top of virtualized hardware. GPU Droplets offer on-demand access to high-powered GPUs to help customers train AI models, process large datasets, and handle complex neural networks.

Volumes Block Storage

Volumes block storage are network-based block devices that provide additional data storage for Droplets. Droplets are moveable and can be resized at any time.

Spaces

Spaces is an S3-compatible object storage service that allows for storage of large amounts of data. Each Space is a bucket to store and serve files. The free, built-in Spaces content delivery network minimizes page load times, improves performance, and reduces bandwidth and infrastructure costs.

PaaS Offerings

Kubernetes

DigitalOcean Kubernetes ("DOKS") is a managed Kubernetes service that allows for the deployment of Kubernetes clusters without the complexities of handling the control plane and containerized infrastructure. Clusters are compatible with standard Kubernetes toolchains and integrate natively with DigitalOcean load balancers and volume block storage.

Managed Databases

Managed Databases are a fully managed database cluster service. Using managed databases is an alternative to installing, configuring, maintaining, and securing databases manually.

App Platform

App Platform allows developers to publish code directly to DigitalOcean servers without having to manage the underlying infrastructure.

App Platform can either automatically analyze and build code from your GitHub, GitLab, or public Git repositories, and publish applications to the cloud or publish a container image already uploaded to the DigitalOcean Container Registry or Docker Hub. It also has lifecycle management features, vertical and horizontal scaling, push-to-deploy support, introspection and monitoring features, built-in database management, and integration.

Container Registry

The DigitalOcean Container Registry ("DOCR") offers the security of a private Docker image registry, with extra tool support that enables easy integration with Docker environments and DOKS clusters. These registries are private and co-located in the data centers where DOKS clusters are operated, to help ensure secure, stable, and performant rollout of images to your clusters.

FaaS Offerings

Functions

Functions are blocks of code configured to run on-demand without the need to manage infrastructure. Functions are designed to allow end users to deploy code that can perform the same tasks as a traditional API without the requirement of configuring a server to manage the requests. Each function that an end user deploys is assigned a unique URL, which the end user can use to anonymously test the function. End users can further invoke their functions and inspect the logs and results directly from their terminal.

Summary of Evaluation Methods and Applicable Articles

Schellman performs one or more of the following testing approaches for each of the certification minimum requirements to validate that DigitalOcean is compliant with the requirements:

1. Inquiry of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related article. This includes in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding. This identifies the control(s) in place to meet the applicable articles.
2. Observe the relevant processes or procedures during fieldwork. This includes, but is not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
3. Inspection of the relevant audit records. This included, but was not limited to, policies, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing may involve tracing events forward to consequent system documentation or processes (e.g. resolution, detailed documentation, alarms, etc.) or backwards for prerequisite events (e.g. approvals, authorizations, etc.).

Explanation of Requirement Classifications

The requirement classifications are defined as follows:

- **Green** – Based on one or more evaluation methods, these requirements are believed to be met.
- **Red** – Based on one or more evaluation methods, the fulfillment of the stated requirement is believed not to be met. This classification is based on the absence of related practices or practices not being designed or implemented properly.
- **Grey** – Based on one or more evaluation methods, the requirement is believed to be not applicable to the organization for the services in scope. If deemed not applicable, rationale should be thoroughly documented and should be reviewed on a periodic basis thereafter to ensure applicability of the requirement has not changed.

DATA PROCESSING AGREEMENT

The below is an excerpt of the data processing agreement detailing the data processing and privacy practices posted to the DigitalOcean website: https://www.digitalocean.com/legal/data-processing-agreement. Should this data processing agreement change prior to the next annual certification assessment, please contact Schellman.

4. International Data Transfer

4.1 If DigitalOcean processes Personal Data of Data Subjects located in the EEA, Switzerland, or the United Kingdom in a country that has not received an adequacy decision from the European Commission or Swiss or UK authorities, as applicable, such transfer shall take place on the basis of DigitalOcean's certification under the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, or the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), as applicable.

4.2 If the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, or the Swiss-U.S. DPF is declared invalid, or if DigitalOcean fails to re-certify for the EU-U.S. DPF, then the transfer of Personal Data will be subject to the Standard Contractual Clauses or UK Addendum, as applicable, which the parties agree will be incorporated by reference into this DPA. The parties agree that, with respect to the elements of the Standard Contractual Clauses and the UK Addendum 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) under Data Protection law, including, if applicable, 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 a 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 only in accordance with Customer's instructions, which instructions comprise: (i) to provide Services to Customer under the Agreement and (ii) comply with applicable law. DigitalOcean will notify Customer if, in DigitalOcean's sole discretion (i) Customer's instruction infringes upon applicable Data Protection Law or (ii) 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 Processed on behalf of Customer 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 or as otherwise required by applicable law. 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 on behalf of Customer in connection with the Services. Upon request, DigitalOcean will provide reasonable 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 under applicable law. 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 (or, upon Customer's request, returned to Customer), 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 audit 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 audit 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; (c) such audit must not unreasonably interfere with DigitalOcean's business activities, must be reasonable in time and scope, and must not cause DigitalOcean to breach its confidentiality obligations to other customers; (d) the parties must agree to a specific audit plan, including confidentiality obligations, prior to any such audit, which must be negotiated in good faith between the parties; and (e) Customer keeps all results of the audit confidential. 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.

SECTION 3

TESTING RESULTS

TESTING RESULTS

#	Requirement	Classification	Classification Comment (with rationale if applicable)
	Security Safeguards		
1.	Implement an information security policy that covers personal information processed on behalf of a controller.	~	Compliant
2.	Implement physical, technical, and administrative safeguards that may include the following and periodically review and reassess the implemented measures to evaluate their relevance and effectiveness: · Authentication and access control (e.g. password protections) · Encryption · Boundary protection (e.g. firewalls, intrusion detection) · Audit logging · Monitoring (e.g. external and internal audits, vulnerability scans)	~	Compliant
3.	Implement regular training and oversight of employees to ensure they are aware of the importance of, and obligations for, respecting and maintaining the security of personal information.	~	Compliant
4.	Implement measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information. The measures implemented should be tested on a periodic basis and measures should be adjusted to reflect the results of the tests.	~	Compliant
5.	Implement a notification process to notify the controller of occurrences of a breach of the privacy or security of their organization's personal information.	~	Compliant
6.	Implement procedures for the secure disposal or return of personal information when instructed by the controller or upon termination of the relationship with the controller.	~	Compliant
7.	Perform periodic third-party certifications or other risk assessments and adjust the security safeguards to reflect the results of these certifications or risk assessments.	~	Compliant
	Accountability		
1.	Implement policies to ensure that processing of personal information is limited to the purposes specified by the controller.	~	Compliant
2.	Implement procedures to delete, update, and correct information upon request from the controller where necessary and appropriate.	~	Compliant

#	Requirement	Classification	Classification Comment (with rationale if applicable)
3.	Implement measures to ensure compliance with the controller's instructions related to the activities of personal information processing.	~	Compliant
4.	Appoint an individual(s) to be responsible for the overall compliance with the requirements of the PRP.	~	Compliant
5.	Implement procedures to forward privacy-related individual requests or complaints to the controller or to handle them when instructed by the controller.	~	Compliant
6.	Implement procedures to notify controllers, except where prohibited by law, of judicial or other government subpoenas, warrants or orders that require the disclosure of personal information.	~	Compliant
7.	Notify the controller of the organization's engagement of subprocessors.	~	Compliant
8.	Implement mechanisms with subprocessors to ensure that personal information is processed in accordance with the organization's obligations under the PRP. Mechanisms should require subprocessors to perform the following: · Follow-instructions provided by the organization relating to the manner in which personal information must be handled · Impose restrictions on further subprocessing · Have the subprocessor's PRP recognized by an APEC Accountability Agent in the subprocessor's jurisdiction · Provide the organization with self-assessments or other evidence of compliance with the organization's instructions and/or agreements/contracts · Allow the organization to carry out regular spot checking or other monitoring activities	~	Compliant
9.	Regularly train employees on the organization's privacy policies and procedures and related client instructions.	~	Compliant