DigitalOcean

2021 DigitalOcean Transparency Report

Introduction

DigitalOcean's mission is to simplify cloud computing so developers and businesses can spend more time creating software that changes the world. We believe that fostering a community based on a foundation of trust is a core value of our services and we take our responsibility of being trusted data stewards very seriously.

As part of our commitment to the privacy of your data, DigitalOcean issues annual reports to provide visibility to the DigitalOcean community regarding requests received for customer information from federal governments and law enforcement agencies across the world. Like many cloud computing companies, we occasionally receive requests from government agencies regarding servers in our network. To protect our customers, our policy is to fully (and transparently) comply with legal processes, provided that it is legally valid and binding with respect to where the data in question resides.

We stand with our customers when governments ask us for data. We don't disclose user data to law enforcement without proper legal process and we inform users about government data requests unless legally prevented from doing so. Our transparency reports outline the requests we receive from law enforcement agencies and explain our commitment to being responsible cloud providers.

2021 year in review

This report summarizes government or law enforcement requests for customer data received between January 1, 2021 and December 31, 2021. We expect to continue to publish these reports annually.

In the 2020 report, we updated how we reported requests for customer data and broke down requests by regions as well as updated our definitions to focus on the types of customer data requested. As a response to the Court of Justice of the European Union's (CJEU) Schrems II decision in 2020, we updated our Data Processing Agreement (DPA) with the use of the New Standard Contractual Clauses (SCCs) and implemented the European Data Protection Board (EDPB) recommendations in regards to technical, organizational, and legal supplementary measures. We continue to proactively monitor for changes to regulations that impact customer data to ensure our security and privacy controls meet our high standards for data protection.

Consistent with last year's report, we've continued our updated reporting of requests for customer data through a breakdown of the requests by the following regions: US, EU, and International.

Unless we are otherwise prohibited from doing so, our policy is to notify customers and provide them with a copy of any legal process regarding their account. The length of non-disclosure orders and process of renewing those orders can extend the delay in notification well beyond the calendar year in which we received the initial request. We regularly evaluate our process to hold law enforcement accountable to renewing or withdrawing non-disclosure orders.

Data

Request	Status	EU	International	US	Total
Preservation	Complied	9	4	129	142
	Did not comply	1	3	36	40
Imminent harm	Complied	1	17	19	37
	Did not comply		2	1	3
Non-content data	Complied	43	44	312	399
	Did not comply	56	74	115	245
	Pending			1	1
PRTT	Complied	1		18	19
	Did not comply			5	5
Content data	Complied	13	4	37	54
	Did not comply			7	7
National Security requests				*0-249*	
Grand total		**124**	**148**	**680**	**952**

Percentage of requests by country