2020 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 one of the 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 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.

2020 YEAR IN REVIEW

This report summarizes government or law enforcement requests for customer data received between January 1, 2020 and December 31, 2020. We expect to continue to publish these reports annually.

In the 2019 report, we focused on the expansion of our Transparency Report to cover law enforcement agencies beyond the United States where our data centers are located. A notable development in 2020 was the Court of Justice of the European Union's (CJEU) decision to invalidate Privacy Shield as a legal mechanism for organizations to transfer EU personal data to the US. We quickly responded with the use of Standard Contractual Clauses (SCCs) and review of the European Data Protection Board (EDPB) draft recommendations in regards to technical, organizational, and legal supplementary measures. We proactively monitor for changes to regulations that impact customer data to ensure our security and privacy controls meet our high standards for data protection.

CONTINUED ›

To better reflect the growing changes in the privacy landscape, we've updated how we're reporting requests for customer data and have now provided a breakdown of the requests by the following regions: US, EU, and International. We also updated our definitions to focus on the types of customer data requested.

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. In future transparency reports, we plan on providing metrics on the volume of requests received with non-disclosure orders or provisions attached, and the percentage of eligible customer accounts notified.

DATA

Request	Status	EU	INTL	US	Total
Non-content Data	Complied	11	17	314	342
	Did Not Comply	42	103	143	288
	Pending		1	4	5
Content data	Complied	13	2	27	42
	Did Not Comply	1		20	21
	Pending	2		2	4
PRTT	Complied			19	19
	Did Not Comply			3	3
Imminent harm	Complied	4	21	20	45
	Did Not Comply	1	2	3	6
Preservation	Complied	4	5	146	155
	Did Not Comply	2	2	24	28
	Pending			1	1
National Security Requests				0-249	
Grand Total		**80**	**153**	**726**	**959**

PERCENTAGE OF REQUESTS BY COUNTRY

United States: 76.8%
Other: 7%
Canada: 1.9%
India: 8.1%
Germany: 4.4%
Singapore: 1.8%