VULTR

Vultr Security and Compliance

Building trusted cloud infrastructure by putting security and compliance at the heart of our mission.

VULTR.COM

Vultr Security and Compliance

Security first. Privacy first. Customer first.

Vultr delivers enterprise-grade composable cloud infrastructure with global reach and unmatched price-to-performance. When designing our services, your security and privacy are our foremost priorities.

Vultr is dedicated to ensuring our platform, products, and services meet the diverse global compliance, privacy, and security needs of our customers, covering areas such as server availability, security, data protection, and privacy. Our commitment to aligning to industry-wide privacy and security frameworks is demonstrated through our CSA Star Level I assessment (CAIQ) and our SOC 2 Type 2 attestation, verified by independent third-party auditors, and our ongoing adherence to the SOC 2 framework. We have also been audited to comply with several crucial ISO and PCI certifications, including PCI Merchant for user data protection.

Vultr's cloud services are designed with compliance in mind, allowing our customers to deploy solutions tailored to their specific compliance requirements, including HIPAA, ISO, PCI, SOC, and others. By aligning with the compliance frameworks of our data centers, customers can leverage a comprehensive compliance playbook to implement the necessary controls for their environment.

Vultr's attestations and certifications

Vultr has successfully attained the following attestations and certifications:

- SOC 2 Type 2
- CSA Star Level 1
- ISO 20000
- ISO 27001
- PCI (Merchant)

We are actively expanding our compliance attestations and certifications. The following certifications are scheduled for completion in the near future:

- ISO/IEC 27017:2022
- ISO 27018:2022
- FedRAMP
- PCI Service Provider
- MeiTy

Data privacy

Since our inception, Vultr has been committed to upholding and adhering to the strictest data privacy and protection standards worldwide, including HIPAA, GDPR, LGPD, DPDPA, US privacy laws, and data sovereignty laws.

Vultr's collection of personal data is limited by our privacy policy, which only includes the information required to provide our services and communicate with you. User content data, such as on websites or online services built on Vultr's infrastructure, are not included in this agreement, and Vultr serves solely as a data processor (service provider). Vultr does not claim any rights to, use, access, allow access to, or share your content other than as may be required by law or for security purposes.

Additionally, Vultr's data sovereignty options ensure that data remains within selected regions and is not processed in other locations or jurisdictions.

Separation of responsibilities

■ **You manage**   ■ **Provider managed**

Infrastructure as a Service

Applications	Data	Runtime	Middleware	O/S	Virtualization	Servers	Storage	Networking

Platform as a Service

Applications	Data	Runtime	Middleware	O/S	Virtualization	Servers	Storage	Networking

GDPR and DPDPA compliance

Vultr's processes have gone through an extensive procedural and legal review to ensure we fully meet the requirements set forth in the EU General Data Protection Regulation (GDPR) legislation and in the India Data Protection and Digital Privacy Act (DPDPA).

If GDPR or DPDPA applies to your organization and you need a DPA, Vultr will provide it upon request.

Compliance with other data standards

Vultr's services are also compliant with further data privacy and protection regulations, including:

- California's Consumer Privacy Act (CCPA)
- Brazil's Lei Geral de Proteção de Dados (LGPD)
- India Data Protection and Digital Privacy Act (DPDPA)
- U.S. State level regulations in CA, CO, CT, DE, FL, IN, IA, MT, NJ, OR, TN, TX, UT, and VA

Vultr's commitment to HIPAA compliance is delivered through Business Associate Agreements with our customers and service providers. Vultr also ensures HIPAA customers are deployed at data centers with the HiTrust certification.

Shared responsibility model

At Vultr, we recognize that security and compliance are shared responsibilities among us, our customers, and any third-party providers involved in delivering products or services. While Vultr manages and secures the platform's control plane, networks, and cloud storage, our data centers handle physical security controls, and customers are responsible for their applications, data, middleware, operating systems, and storage.

Our rigorous risk management policy requires assessments of all third-party vendors, and our vendor management program maintains stringent policies, processes, and controls to assess all third parties involved in delivering Vultr products or marketplace services.

When customers utilize Vultr alongside products and services provided by our data centers, service providers, and vendors, they benefit from a compliance-focused solution that aligns with various frameworks and regulations, streamlining compliance efforts and alleviating the burden of implementing redundant controls.

Learn more about Vultr Security and Compliance

Contact us at **vultr.com** to get started. →

Data center compliance

Data center	SOC 1 Type 2	SOC 2 Type 2	ISO 27001	PCI-DSS	NIST 800-53	HITRUST
Amsterdam		✓	✓	✓		
Atlanta	✓	✓	✓	✓		✓
Bangalore	✓	✓				
Chicago		✓				
Dallas		✓	✓	✓		
Delhi NCR	✓	✓				
Frankfurt		✓	✓	✓		
Honolulu	✓	✓				
Johannesburg	✓		✓			
London		✓	✓	✓		
Los Angeles	✓	✓	✓	✓	✓	✓
Madrid	✓	✓	✓	✓		
Manchester	✓	✓	✓	✓		
Melbourne	✓	✓	✓	✓		
Mexico City	✓	✓	✓	✓		
Miami	✓	✓	✓	✓	✓	✓
Mumbai	✓	✓	✓	✓		
New Jersey	✓	✓	✓	✓		✓
Osaka	✓	✓	✓	✓		
Paris		✓	✓	✓		
San Jose	✓	✓	✓	✓	✓	✓
Santiago		✓		✓		
Sao Paulo	✓	✓	✓	✓		
Seattle	✓	✓	✓	✓		
Seoul	✓	✓	✓	✓		
Silicon Valley	✓	✓	✓	✓	✓	✓
Singapore	✓	✓	✓	✓		
Stockholm	✓	✓	✓	✓		
Sydney	✓	✓	✓	✓		
Tel Aviv			✓	✓		
Tokyo	✓	✓	✓	✓		
Toronto	✓	✓	✓	✓	✓	
Warsaw	✓	✓	✓	✓		

VULTR