Security & Compliance Overview

Customer Trust and Data Security are at the Core of Everything We Do at Alive5

Data Center & Network Security

Alive5 is hosted within AWS. Amazon Web Services (AWS) is the world's most comprehensive and broadly adopted cloud platform, offering over 200 fully featured services from data centers globally. Millions of customers - including the fastest-growing startups, largest enterprises, and leading government agencies - are using AWS to lower costs, become more agile, and innovate faster.

Compliance

Alive5 has established compliance with SOC2 Type II, GDPR, CCPA, and PCI-DSS. Additional details and related documentation can be furnished upon request by emailing us at compliance@alive5.com.

Privacy

As part of our commitment to protecting your privacy and your rights to data protection, we collect, process, and store your personal data.

Call or Text 1-855-551-8858
support@alive5.com

DATA CENTER & NETWORK SECURITY

Our Datacenter

We're hosted within Amazon Web Service (AWS) data center. Our servers are in a virtual private cloud (VPC) protected by network access control lists (ACLs) to prevent unauthorized access.

Data in Transit

All Alive5 connections are hosted over HTTPS. HTTPS stands for HTTP over SSL/TLS, a secure form of HTTP that is supported by all major browsers and servers. All HTTP requests and responses are encrypted before being sent across a network. HTTPS combines the HTTP protocol with symmetric, asymmetric, and X.509 certificate-based cryptographic techniques. HTTPS works by inserting a cryptographic security layer below the HTTP application layer and above the TCP transport layer in the Open Systems Interconnection (OSI) model. The security layer uses the Secure Sockets Layer (SSL) protocol or the Transport Layer Security (TLS) protocol.

Encryption & Data Storage

All user data stored in Alive5 is fully encrypted at rest. Encryption at rest provides enhanced security by encrypting all your data at rest using encryption keys stored in our datacenter.. This functionality helps reduce the operational burden and complexity involved in protecting sensitive data. With encryption at rest, you can build security-sensitive applications that meet strict encryption compliance and regulatory requirements.

Encryption at Rest

We encrypt data using industry-standard AES-256 algorithms, which ensure that only authorized roles and services can access sensitive data with access to the encryption keys audited by AWS services.

Encryption in Transit

Traffic is encrypted in transit using Transport Layer Security 1.2 (TLS) with an industry-standard AES-256 cipher. We are also PCI-DSS compliant with our AlivePay tool.

SAML Single Sign On (SSO)

Through SSO, you can authenticate users in your own systems without requiring them to enter additional login credentials.

Call or Text 1-855-551-8858
support@alive5.com

COMPLIANCE

SOC2 TYPE II

Alive5 is SOC2 Type 2 compliant. Developed by the American Institute of CPAs (AICPA), SOC 2 defines criteria for managing customer data based on five “trust service principles”—security, availability, processing integrity, confidentiality and privacy. Alive5 has undergone SOC2 audits from external 3rd party security firms to achieve compliance. An annual report can be furnished upon request with a signed NDA. Please email us at compliance@alive5.com to start the process.

PCI DSS

All payment and PCI data requests go through our partner, PCI Booking. To receive a copy of the latest Attestation of Compliance (AOC) please email us at compliance@alive5.com.

Call or Text 1-855-551-8858
support@alive5.com

PRIVACY

GDPR / Privacy Shield

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU). Since the Regulation applies regardless of where websites are based, it must be heeded by all sites that attract European visitors, even if they don't specifically market goods or services to EU residents.

For Alive5, GDPR details can be referenced within our Privacy Policy at: https://www.alive5.com/privacy-policy, Section 8. Additionally, our participation in the Privacy Shield Framework can be found: https://www.privacyshield.gov/participant?id=a2zt0000000TNY1AAO&status=Active

CCPA

The California Consumer Privacy Act of 2018 (CCPA) gives consumers more control over the personal information that businesses collect about them and the CCPA regulations provide guidance on how to implement the law. This landmark law secures new privacy rights for California consumers, including:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale of their personal information; and
- The right to non-discrimination for exercising their CCPA rights.
- Businesses are required to give consumers certain notices explaining their privacy practices. The CCPA applies to many businesses, including data brokers.
- For Alive5, CCPA details can be referenced within our Privacy Policy at: https://www.alive5.com/privacy-policy, Section 13.

Call or Text 1-855-551-8858
support@alive5.com