Verigo
Truth in Transit
747 SW 2nd Ave
IMB 28 Suite 227
Gainesville, FL 32601
United States

MARCH 24, 2017

VERIGO DATA PRIVACY STATEMENT

Verigo Statement

Verigo utilizes Amazon Web Services (AWS) for data storage. AWS is recognized as an industry leader in cloud services, including data storage. At Verigo, we understand the importance of our customers' data security. Through secure AWS servers, only authorized company users are provided access to confidential information.

VERIGO ENCRYPTION

- All communication between users and the Verigo Cloud is encrypted using Transport Layer Security (TLS) and/or Secure Socket Layer (SSL).
- User credentials are encrypted using a one-way salted hashing algorithm.
- We urge all Verigo users to practice safe security procedures for credential maintenance.

Amazon Web Services Statement: As-of March 12th, 2019

DATA PRIVACY

At AWS, customer trust is our top priority. We deliver services to more than one million active customers, including enterprises, educational institutions, and government agencies in over 190 countries. Our customers include financial services providers, healthcare providers, and governmental agencies, who trust us with some of their most sensitive information.

We know customers care deeply about privacy and data security. That's why AWS gives customers ownership and control over their customer content by design through simple, but powerful tools that allow customers to determine where their customer content will be stored, secure their customer content in transit or at rest, and manage access to AWS services and resources for their users. We also implement responsible and sophisticated technical and physical controls designed to prevent unauthorized access to or disclosure of customer content.

Verigo
Truth in Transit

747 SW 2nd Ave
IMB 28 Suite 227
Gainesville, FL 32601
United States

Maintaining customer trust is an ongoing commitment, we strive to inform customers of the privacy and data security policies, practices and technologies we've put in place. These commitments include:

Ownership and Control of customer content:

- Access: Customers manage access to their customer content and AWS services and resources. We provide an advanced set of access, encryption, and logging features to help you do this effectively (such as AWS CloudTrail). We do not access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users.

- Storage: Customers choose the region(s) in which their customer content will be stored. We will not move or replicate customer content outside of the customer's chosen region(s), except as legally required and as necessary to maintain the AWS services and provide them to our customers and their end users.

- Security: Customers choose how their customer content is secured. We offer our customers strong encryption for customer content in transit or at rest, and we provide customers with the option to manage their own encryption keys.

- Disclosure of customer content: We do not disclose customer content unless we're required to do so to comply with the law or a valid and binding order of a governmental or regulatory body. Unless prohibited from doing so or there is clear indication of illegal conduct in connection with the use of Amazon products or services, Amazon notifies customers before disclosing customer content so they can seek protection from disclosure.

- Security Assurance: We have developed a security assurance program using global privacy and data protection best practices in order to helping customers establish, operate and leverage our security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments.

Adam Kinsey

Adam Kinsey
iOT Solutions Global Sales Lead