articulate

Global Data Security and Privacy at Articulate

This document was updated in October 2026.

Articulate 360 is a learning intelligence platform that helps organizations turn what they know into what their people can do. It includes Articulate 360 AI for learning and development (L&D) teams and Frontline for teams across the business who create training. Together, they combine modern creation formats, AI grounded in learning science, and enterprise-grade admin and security controls, so training builds real capability and scales consistently across the organization.

You may have questions about how we keep your data safe across our products. At Articulate, we understand the importance of protecting our customers' data. That's why we have implemented comprehensive technical and organizational security measures to ensure the confidentiality, integrity, and availability of our systems and services.

This customer assurance all begins with our adherence to key regulatory frameworks for compliance, hosting and disaster recovery, encryption and data protection, data management, data privacy, AI, and hiring and training practices. Learn more in the sections below.

Compliance

Articulate is committed to complying with the highest standards for data security and privacy practices. Certifications from global industry leaders such as the American Institute of Certified Public Accountants (AICPA), the International Organization for Standardization (ISO), and the Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) program reflect our dedication to maintaining high data security and privacy standards.

Here is a list of the current global certifications that we hold:

- ISO 27001 (Information Security)
- ISO 27701 (Data Privacy)
- ISO 42001 (Artificial Intelligence)
- AICPA's SOC2 Type 2 (Trust Service Principles: Security, Availability, and Confidentiality)
- Cloud Security Alliance's CSA Star Level 1

Articulate has certified our adherence to the EU-U.S. Data Privacy Framework and Swiss-U.S. Data Privacy Framework, along with the UK Extension (together, the "DPF Program"), regarding the transfer of personal data from the EEA and Switzerland to the United States. To learn more about the DPF program and to view our certification, please visit https://www.dataprivacyframework.gov/s. In addition, Articulate has taken measures to align with the General Data Protection Regulation (GDPR) by using EU-approved Standard Contractual Clauses for all EU-based customers. We've also aligned with other global privacy laws, including those in the United Kingdom, South Korea, Australia, and Brazil. For more information about our data privacy practices, please visit the Articulate Trust Center.

Hosting and Disaster Recovery

Articulate uses Amazon Web Services (AWS) as its hosting provider with a US data center in northern Virginia and an EU data center in Germany. Articulate 360 services are redundant across at least three isolated and resource-independent availability zones. This redundancy ensures that up to two data centers can go offline simultaneously while we continue to provide customers with a great experience. You can learn more about our services' uptime by visiting https://www.articulatestatus.com.

Articulate's infrastructure exists as a virtual environment and is entirely scalable. Capacity monitoring is performed to ensure that resource usage (including available storage) stays within acceptable limits. We can also accommodate any additional capacity needs quickly through Amazon Web Services (AWS).

The Platform Engineering team performs frequent, fully automated customer data backups with up-to-the-minute recovery options. They also conduct nightly data recovery testing with full automation and monitoring to identify issues during backup production or test restoration. This reduces the likelihood of data loss and minimizes downtime during large-scale disasters. Backup data is isolated from production systems and redundantly stored across multiple Availability Zones in AWS us-east-1 (Northern Virginia) or eu-central-1 (Frankfurt), depending on where the customer's subscription resides.

Encryption and Data Protection

Articulate leverages Amazon Web Services' (AWS) Key Management Service (KMS) to manage the life cycle of keys within our AWS environment. KMS is natively supported by AWS services and backed by hardware security modules (HSMs).

Access to the KMS management console is restricted to approved Articulate personnel with role-based business needs only.

Articulate uses the latest encryption technology to secure all customer data and supports customer data encryption Transport Layer Security protocols 1.2 and 1.3 encryption methods for data in transit. Data at rest on our servers is encrypted using industry standards (e.g., AES 256).

Data Management

Articulate engineers are given limited access to customer content to troubleshoot production outages. A small subset of our engineering team has full access to production infrastructure with safeguards in place, including two-factor authentication and short-leased, revocable sessions.

Our engineers use individual user accounts, each with a two-factor authentication requirement. A secure channel (VPN) and username/password authentication are required for all remote access to Articulate information and systems. All access to our AWS infrastructure is logged for auditing purposes.

These practices are audited annually as part of our SOC 2 Type 2 Audit.

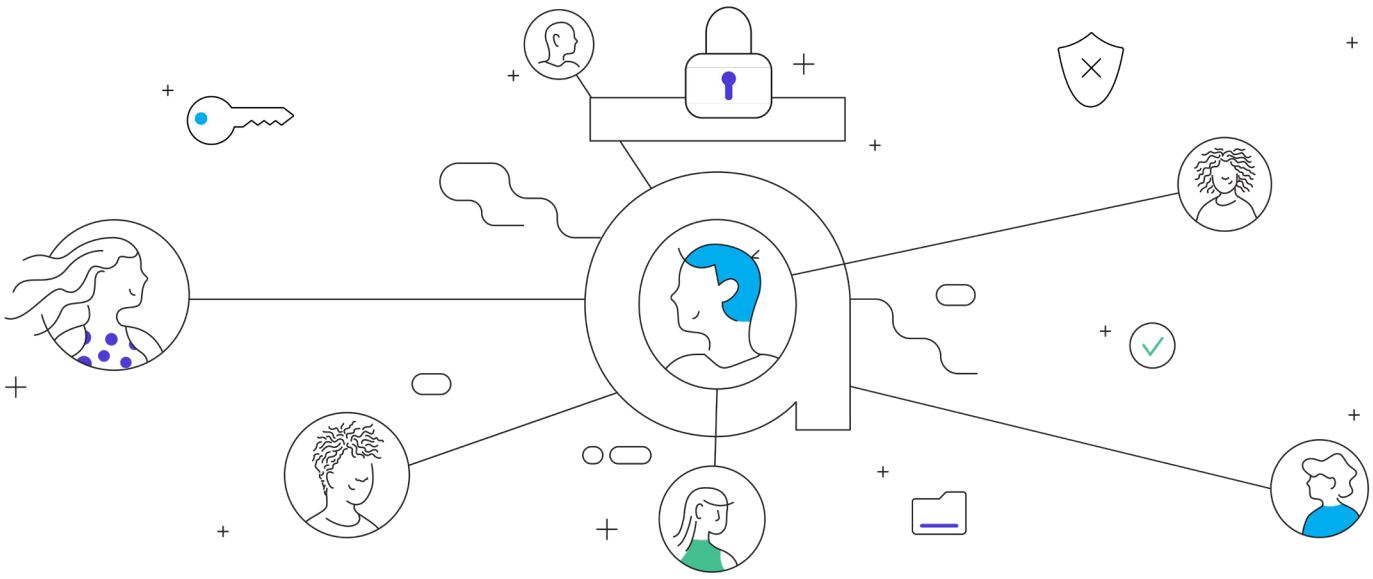
Data Privacy / GDPR

At Articulate, we value our worldwide customer base and your right to privacy.

Under the GDPR, if you are an employee or one of our customers' users, we are generally considered a data processor: We collect data as we deliver services to our customers, who are considered data controllers. We engage carefully vetted subprocessors for specific purposes to provide e-learning services.

We require that each subprocessor agree to a Data Processing Agreement (DPA) that reflects our commitment to take data privacy obligations seriously.

Providing you with control over Articulate's collection, retention, and usage of your data is a vital component of the GDPR. For more information about how we align with the GDPR, please visit the Articulate Trust Center - Learn How We Comply with GDPR.



Artificial Intelligence

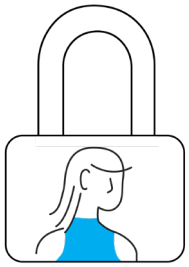
Articulate 360 includes features powered by artificial intelligence (AI) that are designed to help you create and deliver training more efficiently. These features are governed by our AI Responsible Use Policy and operate within our ISO/IEC 42001:2023-certified AI management system, the international standard for the responsible governance of AI.

Customer content processed by our AI features is not used to train third-party foundation models. AI processing follows the same encryption, access control, and regional hosting standards described throughout this document, and all subprocessors supporting these features are subject to the same Data Processing Agreement requirements as our other subprocessors.

For detailed information about our AI architecture, security controls, and data handling practices, please visit the Articulate Trust Center, where you'll find our AI Technical Architecture, AI Security and Privacy Whitepaper, and AI Detailed Security FAQ.

Hiring and Training Practices

Articulate hires top engineers with proven industry track records to maintain our infrastructure. In addition, we provide ongoing internal and external training opportunities. Security engineers are provided content and trained on security-specific processes and knowledge relevant to our security program.



We take data security and privacy very seriously. Our commitment to maintaining the highest standards for data protection ensures that our customers' data is always protected.

If you have any questions regarding our data security and privacy practices, please contact us at security@articulate.com.



Copyright ©2026 Articulate Global, LLC. All rights reserved.
Articulate and all other trademarks mentioned in this document are the property of their respective owners.