

WalkMe Security Compliance

Brief Overview

WalkMe is the Digital Adoption Platform pioneer and leads the industry standard for security and compliance. WalkMe complies with both GDPR and CCPA in WalkMe's services to its customers.

You can find more about WalkMe's privacy policies, compliance standards, and certifications below.

Note

As much of this documentation is confidential, some require login for access.

Security

Datasheet

Below is a highly technical document covering key aspects of the WalkMe security datasheet.

[WalkMe Security Datasheet](#)

WalkMe Security, Privacy, & Architecture

Below is the WalkMe Security, Privacy, & Architecture White Paper document. This is an informational document issued by WalkMe to introduce WalkMe's security, privacy, and architecture.

[WalkMe White Paper - Security, Privacy, & Architecture](#)

WalkMe DAP Solution Overview

Below is the WalkMe DAP Solution Overview White Paper document. This is an informational document issued by WalkMe to promote and highlight the features of our solution.



[WalkMe White Paper - DAP Solution Overview](#)

Privacy

WalkMe Data

Below is a highly technical document listing exactly what is being tracked in Insights in all different tracking modes.

[WalkMe Data Collected Whitepaper](#)

Data Protection

WalkMe complies with GDPR as a data processor CCPA as a Service Provider in the provision of WalkMe's services to its customers and can make its Data Processing Addendum (DPA) available for execution. In addition, we are devoted to helping our customers with their GDPR and CCPA compliance processes by providing robust privacy and security protections built into our services and contracts.

By default, WalkMe does not collect personally identifiable information (PII) other than IP addresses in logs for security purposes, end-users' approximate geolocation (country and city in which they are located) and masked IP addresses for the ongoing operation of the WalkMe system, and assigns collected metadata to anonymous random GUID. Moreover, WalkMe collects and transfers environment properties such as browser and OS, page URL, and title.

the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act set national standards for the privacy and security of electronically protected healthcare information.

[WalkMe Data Protection Overview](#)

Data Protection Framework

The EU-U.S. DPF, UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF were respectively developed by the U.S. Department of Commerce and the European Commission, UK Government, and Swiss Federal Administration to provide U.S. organizations with reliable mechanisms for personal data transfers to the United States from the European Union, United Kingdom, and Switzerland while ensuring data protection that is consistent with EU, UK, and Swiss law.

[Learn More](#)

Certification

ISO 27001 Information Security Certification

WalkMe received the International Organization for Standardization Certification for Information Security (ISO 27001:2013). The audit evaluated WalkMe's information security management system from the product, infrastructure, and organizational aspects, and verified that WalkMe has the necessary information security controls in place to ensure the confidentiality, integrity, and availability of sensitive information assets.

[View Here](#)

ISO 27701 Privacy

ISO/IEC 27701:2019 is a privacy extension to ISO/IEC 27001. The design goal is to enhance the existing Information Security Management System (ISMS) with additional requirements in order to establish, implement, maintain, and continually improve a Privacy Information Management System (PIMS). The standard outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage privacy controls to reduce the risk to the privacy rights of individuals.

[View Here](#)

ISO 27017 Cloud Specific Control

ISO 27017 provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27002 and ISO 27001 standards. This standard provides additional information security controls implementation guidance specific to cloud service providers. WalkMe's attestation to the ISO 27017:2015 guidance demonstrates our ongoing commitment to align with globally recognized best practices and verifies that WalkMe has a system of highly precise controls in place that are specific to our cloud services.

[View Here](#)

ISO 27018 Personal data Protection (PII)

ISO 27018 is a standard that focuses on the protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to public cloud personally identifiable information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO 27002 control set. WalkMe customers can know where their data is stored.

Customer data won't be used for marketing or advertising without explicit consent.

[View Here](#)

ISO 27799 Security management in health (PHI)

ISO 27799 gives guidelines for organizational information security standards and information security management practices including the selection, implementation, and management of controls in health informatics of ISO/IEC 27002 and is a companion to that International Standard.

[View Here](#)

ISO 27032 Guidelines for Cybersecurity

WalkMe is ISO/IEC 27032 certified for Guidelines for Cybersecurity. ISO/IEC 27032:2012 provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on information security, network security, internet security, and critical information infrastructure protection (CIIP) domains

[View Here](#)

ISO/IEC 20243:2018 (O-TTPS) for Mitigating maliciously tainted and counterfeit products (Supply Chain security management)

WalkMe is ISO/IEC 20243:2018 (O-TTPS) certified for Mitigating maliciously tainted and counterfeit products (Supply Chain security management). ISO/IEC 20243:2018 is applicable to WalkMe LTD's Digital Adoption Platform Supply chain security management to meet ISO/IEC 20243-1:2018 Open Trusted Technology Provider (O-TTPS) standard requirements. The scope applies to the entire organization and consists of provisioning software, configuration, implementation, and services to



include delivery of products, services and solutions to our federal government, state and local and commercial customers globally.

[View Here](#)

STAR Certification

WalkMe also achieved a STAR Certification from the Cloud Security Alliance (CSA). STAR Certification is an internationally recognized cloud security certification program jointly developed by CSA and BSI, that specifies comprehensive and stringent cloud security requirements for software vendors.

[View Here](#)

Accessibility Statement of Compliance

WalkMe was given a Accessibility Statement of Compliance from UserWay stating that WalkMe is compliant with the ADA and Section 508 requirements for website accessibility based on WCAG 2.1 AA.

[View Here](#)

Reports

Service Organization Control 2 Type II - Security, Availability, & Confidentiality Report

WalkMe completed a Service Organization Control (SOC) 2 Type II audit, which is one of the most stringent international standards for security, availability, processing integrity, confidentiality, and privacy. Our commitment to the SOC 2 Type II report is ongoing and periodic audits are performed on a regular basis. Available only with NDA.

WalkMe SOC 2 Report is available to WalkMe customers with signed NDA. Please [log-in](#) to access this document.

[View Here](#)



Service Organization Control 3 Type II - General Controls Report

We have a SOC 3 Type II General Use Report, demonstrating that WalkMe has met the AICPA auditable trust services principles (security, availability, processing integrity, confidentiality, and privacy), which is publicly available for free distribution without prior need for NDA.

[View Here](#)

Skyhigh CloudTrust™

WalkMe's Digital Adoption Platform was awarded the highest Skyhigh CloudTrust™ rating of Enterprise-Ready™ by fulfilling a comprehensive set of requirements for data protection, identity verification, service security, business practices, and legal protection.

[View Here](#)

Standardized Information Gathering (SIG)

WalkMe completed the 2017 Standardized Information Gathering (SIG) Questionnaire, administered by The Santa Fe Group.

[View Here](#)

CSA

WalkMe completed the Consensus Assessments Initiative Questionnaire (CAIQ) organized by CSA to assist in general principles of cloud security.

[View Here](#)

WalkMe GxP Position Paper

This whitepaper provides guidance for using WalkMe products in the context of GxP and the content has been developed in conjunction with WalkMe pharmaceutical and medical device customers, as well as software partners, who are currently using WalkMe products in their validated GxP systems.

[View Here](#)

AWS Partner Network

For customers, the AWS Partner Network makes it easy to find top APN Partners who:

- With our partnership for AWS customers, are given prioritization over development tasks
- Possess extensive experience building and deploying customer solutions that are built on or integrated with AWS.
- Provide well-architected solutions for AWS customers.
- Develop and retain a strong bench of AWS trained and certified experts.

[View Here](#)

WalkMe Player Voluntary Product Accessibility Template (VPAT™)

This report covers the degree of conformance for the following accessibility standard/guidelines:

- [Web Content Accessibility Guidelines 2.0](#)
- [Web Content Accessibility Guidelines 2.1](#)

[View Here](#)

WalkMe Editor Voluntary Product Accessibility Template (VPAT™)

This report covers the degree of conformance for the following accessibility standard/guidelines:

- [Web Content Accessibility Guidelines 2.0](#)
- [Web Content Accessibility Guidelines 2.1](#)

[View Here](#)