WalkMe and the Applicable Data Protection Legislation

As a global company, WalkMe and its affiliates (“WalkMe”) are required to meet a broad range of international data protection legislation regarding the collection, processing, and retention of personal data of WalkMe’s prospects, customers and business partners. In that respect, the European Union’s General Data Protection Regulation (“GDPR”) and the California Consumer Privacy Act (“CCPA”), and certain other data legislation may apply when engaging with WalkMe’s services and products. The applicability of any of the foregoing data protection legislation is determined on the basis of the jurisdiction in which the end users of the WalkMe Services are residing. As such, if there are end users located in the European Union, the principles of the GDPR apply.

All applicable data protection legislation have in common their ability to enhance individuals’ data privacy rights (“data subjects”) by ensuring greater accountability and transparency regarding why, how and where personal data processing is taking place. As such, WalkMe is dedicated to comply with all applicable data protection legislation through its privacy data protection and security safeguards as further described herein.

Subject to the GDPR, WalkMe is considered the “Data Processor”, whereas, under the CCPA, WalkMe is qualified as a “Service Provider”, as in both instances, the customer is the entity determining the means and purposes of the processing. Before any personal data processing will take place, WalkMe and its customers will enter into a Data Processing Agreement (“DPA”), providing the relevant legal basis and documented instructions for such processing. Moreover, the DPA sets forth the specific details of the types of personal data to be processed.

WalkMe's Personal Data Protection Compliance

WalkMe is devoted to continuously monitoring and updating its services, products, and the accompanying terms, policies, contracts, and documentation in order to enable WalkMe's compliance with the applicable data protection legislation. WalkMe's privacy policy (available at: https://www.walkme.com/privacy-policy/) provides transparency to its customers and end users regarding the personal data collected through their engagement with WalkMe's services and sets forth certain customer rights to enforce their available rights under the applicable data protection legislation.

WalkMe has a robust set of technical security measures in place that meet the highest standards in the industry (for a detailed overview please see: https://www.walkme.com/walkme-security/).

WalkMe implements, enforces and maintains security policies to prevent the unauthorized or accidental access to or destruction, loss, modification, use or disclosure of personal data and monitors its compliance with such policies on an ongoing basis.

All personal data is stored with logical separation from personal data of other customers and only trained and qualified personnel are allowed to process such data subject to strict confidentiality obligations.

Unless otherwise agreed with the customer, and subject to applicable law, WalkMe shall act in accordance with its policies to promptly notify the customer in the event that any personal data processed by WalkMe on behalf of a customer has been lost, stolen, or if there has been any unauthorized access to it. We use a combination of processes, technologies, and physical security controls to help protect personal information from unauthorized access, use, or disclosure. When personal information is transferred over the Internet or stored, we encrypt it using Transfer Layer Security (TLS) encryption or similar technology. Each server is protected by a firewall, exposing it only to the minimum amount of ports necessary.

Certifications

WalkMe has and shall maintain, to the extent applicable, the following certifications:

- ISO 27001:2013 Information Security Certification; The ISO 27001:2013 audit (i) evaluates WalkMe's information security management system for WalkMe's products, infrastructure and organization; and (ii) verifies that all information security controls are in place to ensure confidentiality, integrity and availability of personal information.

- Service Organization Control Type II (SOC2): The SOC 2 technical audit requires companies storing customer data in the cloud to establish and follow strict information security policies and procedures, encompassing the security, availability, processing, integrity, and confidentiality of customer data. SOC 2 ensures that a company's information security measures are in line with the unique parameters of today's cloud requirements;

- EU-U.S. and Swiss-U.S. Certifications: The EU-U.S. and Swiss-U.S. Privacy Shield frameworks provide companies with a mechanism to comply with data protection requirements when transferring personal data from the EU and Switzerland to the United States.

- TrustArc (formerly TRUSTe) Certified Privacy and Third-Party Dispute Resolution Provider: TrustArc validates the appropriateness and completeness of privacy policies and practices in accordance with applicable law and regulation, including EU-U.S. Privacy Shield requirements and provides third-party dispute resolution services for resolution of privacy and data concerns.

- Skyhigh CloudTrustTM: WalkMe was awarded the Skyhigh CloudTrustTM rating of Enterprise ReadyTM by fulfilling a comprehensive set of requirements for data protection, identity verification, service security, business practices, and legal protection.

- STAR Certification from the Cloud Security Alliance (CSA): The STAR Certification is an internationally recognized cloud security certification program jointly developed by CSA and BSI that denotes comprehensive and stringent cloud security;

- Level 1 of Federal Information Process Standard 140-2 (FIPS 140-2): FIPS 140-2 is a security standard for hardware, software and firmware solutions using cryptography in security systems that process sensitive and unclassified information.

Penetration Tests and Monitors

WalkMe's front and back-end applications and IT infrastructure undergo annual penetration tests completed by an independent third-party. WalkMe utilizes the top-tier, secure, cloud services of Amazon Web Services (AWS). AWS undergoes its own independent periodic internal test and 24/7 monitoring of security-related events by the dedicated AWS security teams.

Access Control

WalkMe implements an integrated, comprehensive role-based user management and enforcement system. WalkMe must authorize any assigned roles to users and any permissions are controlled per action and screen with eight (8) roles built into WalkMe's digital adoption platform (DAP) including, without limitation, administrator, content creator, publisher, analytics access, etc. Customers maintain the central management of the deployment of the WalkMe DAP and can delegate usage and administrative permissions in its use of various elements and features of the WalkMe DAP.

Accountability and Security

WalkMe's corporate control access is centrally managed based on strict need-to-know and least-privileged principles on all levels of the system:

- Applications (Strong Authentication);
- Network (Segmentation, Firewall);
- OS (Access To Services);
- Procedural (Authorized to Review/Approve Code, Manage Changes)

Furthermore, WalkMe has an extensive Security Information and Event Management System (SIEM) that collects security audit trail logs across infrastructure components in industry standard formats using an Intrusion Detection System. WalkMe's SIEM alerts are based on comprehensive pre-defined scenarios including identification of suspicious behavior and are monitored 24/7 by WalkMe's Security Operations Center (SOC) team.

Additional Data Protection Compliance Questions

This document provides customers with a brief overview of WalkMe's Data Protection and initiatives. If you have any additional questions regarding WalkMe's data protection, please contact us for further details.