THE CLICKTALE DIFFERENCE

Delivering peace of mind in digital optimization: Clicktale's security standards and practices

CONTENTS

Introduction

Delivering peace of mind

As an enterprise service provider, Clicktale understands that the security of the user data collected and stored by our customers is nothing less than critical. Clicktale's customers include numerous Fortune 500 companies and some of the world's leading financial institutions for whom maintaining secure user data is a top-most priority.

To deliver the peace of mind that our customers deserve, we believe in transparency regarding Clicktale's security standards and practices. This document, created by our dedicated security team, provides an overview of our multi-layered approach to Information Security. Our security practices are constantly evolving to protect against security breaches and provide full confidentiality, data integrity and availability.

As an accreditation for these practices, *Clicktale is ISO 27001 certified, and has been since 2013.* Our certification ensures the highest international standards and best practices in information security.

Privacy and anonymity

Private means private

By design, Clicktale blocks the recording and collection of any Personally Identifiable Information (PII) entered by keystroke, as well as any PII as defined by the customer.

We make great efforts to ensure that data processed by Clicktale on behalf of its clients is completely anonymized.

No PII collected or transmitted

To prevent the collection, saving or display of PII through our products, we have developed a number of implementation tools, including:

- Client-side keystroke block - By default, Clicktale's client-side keystroke block ensures that our product only keeps track of when keys are clicked, without keeping track of which keys are clicked. This helps customers ensure that no keystrokes are logged or recorded by our products, nor sent via the network.

- PII labeling API - Clicktale has developed an API (Application Program Interface) to identify and block any type of PII before it leaves the visitor's browser. This tool enables our customers to easily identify PII fields to maintain the highest levels of data privacy.

- Client-side HTML rewrite rules - When an HTML page is sent directly from the user's browser to Clicktale's servers, any PII in the HTML (as identified by the customer) is removed using standard client-side expressions, before it is sent across the network.

- Server-side HTML block - As a failsafe, Clicktale also offers server-side rewrite rules to remove any PII in HTML as identified by the customer. Thus, even if any PII unintentionally reaches Clicktale's servers, it is removed before it is stored.

- PII exclude block - Customers may also tag sensitive data in the HTML with HTML comments, in order to ensure that any PII in data is removed by the Clicktale parser before being stored on to Clicktale's servers.

No third-party cookies

Clicktale does not use third-party cookies in order to increase user privacy. In other words, Clicktale does not create a unique profile to track users across unrelated domains (domains that do not belong to the same customer). Our opt-out cookie is a third-party cookie, which contains only a Boolean value.

No IP address retention

When a visitor session is complete, Clicktale determines and saves the geographical location of the visitor, but the IP address is deleted. This enables visitors to websites using Clicktale to maintain a high degree of anonymity and privacy.

Clicktale also provides its customers with the option to anonymize the IP address. This is done by removing the D-block of the IP at the earliest possible stage of the collection.

PCI, HIPAA, GLBA

As discussed above, Clicktale takes stringent measures to avoid receiving any personal information from its customers, and as such the data Clicktale processes on behalf of its customers should be completely anonymous. Therefore, Clicktale customers are able to maintain their compliance with PCI, HIPAA and GLBA or similar laws regulating PII.

ISO 27001 compliance

Committed to ISO 27001 certification

ISO 27001 is an international Information Security standard that specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS).

Clicktale is ISO 27001 certified, and has been since 2013. This means that we have developed an ISMS based on security best practices, according to which we implement security controls to protect both our customers' and our own information assets. These controls are systematically evaluated and updated by internal parties and by an external auditor, to ensure that we continually meet both our own information security needs and those of our customers.

Our ISO 27001 certification also means that Clicktale doesn't rely on data center security alone. Whereas other companies may rely solely on the compliance of their SSAE16-certified data center, we ensure that all Clicktale products and internal services go through extensive security controls in order to preserve data confidentiality, integrity and availability.

We view our ISO 27001 certification as an independent assurance to our customers that we have implemented and verified mature security controls for governing the management of customer data.

For more details, visit our ISO 27001 certificate page

Application-level security

Built for security

Clicktale has developed and implemented a strict, secure development program, based on Open Web Application Security Project (OWASP), and Microsoft Security Development Lifecycle. From the earliest phases of product design and planning, the Clicktale security team takes an active role in how our products are built. Following completion, sensitive product developments are tested to ensure that application security has been thoroughly and properly addressed.

On an ongoing basis, security consultants review our code and conduct penetration tests for various attack scenarios based on OWASP and on scenarios relevant specifically to Clicktale. We also conduct extensive secure coding and ethical hacking training for our development and QA teams.

Clicktale utilizes a static code analysis tool to scan our code to detect vulnerabilities during the development process and prior to production.

Our products contain numerous security features, including:

- User authentication - User credentials are transferred via a hypertext transfer protocol secured (HTTPS) connection, a protocol that encrypts communication between the web server and browser and secures web server identification. In addition, user passwords never appear in clear text. We hash each of our user's passwords with unique SALT to ensure that passwords can never be read, not even by us.

- Customizable password policy and session management - Clicktale allows its customers to set users' password length, complexity level, and expiration. Customers can also determine session duration and idle time lockout for its users.

- Account lock-out - To protect against dictionary-based, brute-force attacks, Clicktale user accounts are prompted with a CAPTCHA mechanism after several failed login attempts. If a maximum number of failed logins is exceeded, the account is locked.

- Single sign-on - Clicktale offers enterprise customers authentication via the SAML2 standard. Clicktale's adoption of Security Assertion Markup Language (SAML) enables our customers to control user management and authentication.

- Encryption - Data recorded by Clicktale is encrypted in transit by default on all supporting browsers. In addition, data recorded on HTTPS pages is fully encrypted and passed to Clicktale servers over a TLS connection.

Penetration testing and security audits

Maximizing transparency and trust

Clicktale performs at least two annual Information Security penetration tests, which are conducted by accredited and completely independent information security companies. Vulnerabilities, if found, are addressed as part of our Risk Management Policy.

Clicktale performs vulnerability assessment scanning using third-party tools at least twice a month, and after any major infrastructure change in our production environment.

In addition, Clicktale ensures all external facing certificates are publicly signed and support only the latest and most secure ciphers. A review of SSL certificates is conducted on a weekly basis.

Further to our security team's regular reviews, we conduct an annual Information Security risk assessment to identify new threats, measure their likelihood and business impact, and determine appropriate controls to minimize risk. The results of this assessment are brought to Clicktale's senior management for review and action.

Customer independent tests

Clicktale welcomes customers and potential customers to independently verify our product security by conducting their own vulnerability assessments and penetration tests. Please contact your sales representative in order to coordinate this.

General security overview

Full-time dedicated security team

Clicktale's full-time, dedicated security team is led by our Director of Information Security. Comprised of seasoned information security veterans, the team has far-reaching control over all aspects of data and product security, and is responsible for security training for all Clicktale employees. Through close monitoring of market and information security trends and developments, we continuously improve and update our security policies and practices.

Ironclad information security practices

The Clicktale security team ensures that employees comply with internal data security policies, as well as existing and emerging global and local regulations. Clicktale strives to improve our security practices and processes on a constant basis, ensuring they conform to evolving global and local security standards. Notably:

- Clicktale employees and contractors are contractually committed to adhere to information security policies, procedures, and standards.

- Clicktale has strict security processes for new employees, leaving employees, and employees who move between departments. The processes cover both physical and logical access control privileges and are reviewed regularly.

- Every new Clicktale employee and on-premise consultant receives information security training in the first week of work. Additional training is provided annually to all Clicktale employees.

- Every Clicktale employee or contractor is provided with unique identifiers in order to maintain individual accountability.

- Our user access privileges to information resources are fully compartmentalized and consistent with role-based authorization. Access control exceptions are granted only after the asset owner's formal approval.

- Access to information collected by Clicktale is restricted to a limited number of employees, contractors and agents. These individuals are exposed to sensitive information only for the purpose of providing customers with services and operating, developing or improving Clicktale's products and services. These individuals are bound by confidentiality and non-disclosure agreements and may be subject to disciplinary action, including termination and criminal prosecution if they fail to meet these obligations.

- A review of our access control permissions to sensitive systems is conducted on a quarterly basis.

- Every new third party service goes through a comprehensive information security approval process to maintain supply chain security resilience.

- Clicktale enforces a strong password policy for its internal systems. All password communication is done over secured transmission.

- Clicktale's incident response procedures include a record of security incidents with a description of the event, the time period, the consequences of the event, the name of the reporter, and to whom the incident was reported, as well as procedures for mitigation and lessons learned. Clicktale will also work with customers in the event that a security incident affects their data.

Infrastructure

Safeguarding infrastructure

Clicktale implements multiple and varied infrastructure security measures to protect customer information from unauthorized access, loss, alteration, viruses, Trojans and other similar harmful code. This includes:

- Swift and regular updates of operating systems, hardware, and any third party software to avoid security vulnerabilities. Critical updates are deployed within one week from release on corporate as well as production systems.

- Use of firewalls and Intrusion Prevention Systems (IPS) systems to limit access and protect Clicktale's application.

- Hardening of all external-facing application according to industry best practices.

- Implementing anti-malware controls to prevent entry of malicious software.

- Securing remote access communication using multifactor authentication.

- Backing up customer data on a daily basis, on a rotating schedule.

- All communication between Clicktale's remote locations is conducted via encrypted channels.

Administrative access to our production environment is limited to a restricted number of individuals. Access to additional individuals is given only in extreme circumstances, for a specific purpose, and is limited in duration. Such access to these additional individuals is given only after the explicit approval of the security team.

Clicktale has implemented an advanced Security Incident and Event Management (SIEM) solution to audit, monitor, aggregate, and correlate security alerts, ensuring swift discovery and response to potential security incidents.

Physical premises

Secure data storage facilities

Clicktale has chosen SoftLayer and Amazon Web Services (AWS) as our strategic enterprise data facilities. For detailed information about SoftLayer's security, please click here. For detailed information about AWS, please click here.

All Clicktale client-recorded data is stored on secure servers located in SoftLayer's data center in Texas and in AWS in north Virginia. For European enterprise clients, data is stored in SoftLayer's Amsterdam data center and in AWS in Ireland.

Encrypted backups of our service and client data are stored on the Amazon Web Services cloud.

Physical server security

SoftLayer's data centers and AWS are ISO27001 and SOC2 compliant. Security mechanisms in the data centers include:

- Controlled access and 24-hour security
- 24-hour manned security, including foot patrols and perimeter inspections
- Room monitoring via digital security video surveillance
- Room security via biometric systems
- Strictly limited server-room access to authorized personnel and escorted visitors

Physical redundancy

The data centers provide environmental controls for equipment and data protection, including:

- Fire detection and suppression systems
- Multiple power feeds, fiber links, dedicated generators, UPS Systems, and battery backup
- Power distribution units and electrical panels
- Heating and cooling mechanisms such as CRAC units and chillers

About Clicktale:

Clicktale taps into the wisdom and behavior of millions of visitors so that businesses can deliver the best digital experiences and drive amazing business results. Complex behavioral patterns are synthesized based on millisecond-level actions such as hovers and scrolls, enabling businesses to interpret their customers' digital body language to understand intent. The pioneer in Experience Analytics, Clicktale marries cognitive computing, machine learning and psychological research to automatically surface issues and answer questions that keep executives up at night. With unique behavioral data, clear visualizations, and world-class customer experience expertise, Clicktale is driving the "Experience Era" at the world's leading brands and Fortune 500 companies.
Clicktale. Answer anything.

Global Offices

US: +1 415 651 4291
UK: +44 20 3318 6535

WWW.CLICKTALE.COM