Sogolytics Guarantee: Data Privacy and Security

Introduction

From the Tier-3 data centers that house our data to our rigorous internal and external audits, detailed protocols, and regular trainings, every element of our system is designed to give you complete peace of mind. Whether you're looking for ISO 27001 certification, HIPAA compliance, or GDPR protections, we have you and your data covered.

Many of the world's top companies trust Sogolytics with their most sensitive data, recognizing our commitment to security. We're proud of the certifications and awards we've won, but the trust of our clients is the highest compliment, and we work hard to keep that trust every day.

Security is one of our core values, and securing our customers' data recognizes these standards:

1. All customer data is treated as **private and sensitive**.
2. Customer data is never sold to third parties.
3. Our customers own their own data. While we follow clear and consistent policies for data deletion and retention, customers can opt to follow more intensive protocols.
4. While user experience must be seamless and participation convenient, our architecture prioritizes security while delivering reliable accessibility.

Section 1

User Security

User IDs and Passwords

Sogolytics provides each user in your organization with a unique, secure User ID and password that must be entered each time a user logs on. We follow the best practices in the industry for storing confidential data. Passwords are encrypted in the database before they are saved, and a session "cookie" is issued to record this encrypted authentication information only for the duration of a specific session. The session "cookie" does not include either User ID or password of the user.

Data Ownership

Our customers own all of their survey content and responses. At any point, data may be exported from our system in any available formats for external use.

Closed Accounts

Following account expiry, data is securely stored for one year in the event the account is restored. After a year, the data is completely erased.

Privacy

We have a comprehensive privacy policy that provides a very transparent view of how we handle your data, including how we use your data, who we share it with, and how long we retain it.

Data Residency

All data is stored on servers located in the United States.

Credit Card Security

We do not store any credit card information. Credit card details are securely handled by our completely PCI DSS compliant third-party payment management system.

Section 2

Data Security

Commitment

The security of your survey data is of utmost importance to us, as we know it is to you. We understand it needs to be confidential, accurate, and always available.

Data Encryption in Transit

All our communication is HTTPS. We encrypt data during transit using 256-bit encryption.

Data Center Security

All data center operations are protected 24/7/365 by 6-level security.

Mobile App Security

We follow industry best standards to develop, deploy, authenticate, maintain, and transit data. Any third-party libraries used in the code are thoroughly tested before launch. Informed consent is taken from end-users before collecting or processing information. We do not seek access or auto-store information. User consent is only taken to provide services which absolutely require device permissions or enhance user experience.

Hosting

Sogolytics data is hosted in highly rated data centers, a standard that ensures 24/7 availability, redundancy, and operational sustainability.

Data Center Certification

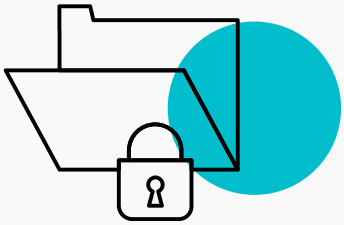
Our hosting data centers are SOC 2 Tier III certified. This extremely stringent rating indicates 99.9% availability for our application users and survey takers, prioritizing experience and security.

Data Center Compliance

The data centers we use have been audited to meet SSAE 16, SAS 70, SOC 2, SOC 3, PCI DSS, and HIPAA compliances.

Section 3

Data Access Control



Two-Step Authentication

Two Step Authentication is a security feature that requires users to authenticate their login using both a password and a time-based one-time password.

Role-Based Access

Control access to your projects, reports, and other data by assigning each user rights to view and/or edit selected content or modules in your account.

Single Sign-On

Sogolytics' Single Sign-On (SSO) feature lets you control login access to your Sogolytics account. SSO removes the hassle of remembering multiple passwords and provides a better user experience. We have implemented SSO using SAML and LDAP, supporting all major SSO technologies.

Section 4

GDPR Compliance

We are fully committed to helping our customers achieve adherence to the General Data Protection Regulation (GDPR). As a result, we have strengthened and standardized our user data privacy across the EU nations in adherence with obligations for all organizations that handle EU citizens' personal data, regardless of where the organizations are located.

GDPR
COMPLIANT

Section 5

Network Security

Firewalls

We follow Minimum Security Baseline (MSB) for system hardening and use a strong firewall for data protection. We follow industry best practices, including ensuring unwanted services are disabled on the firewall, default passwords are changed upon installation, and the firmware version is up to date.

Access Management

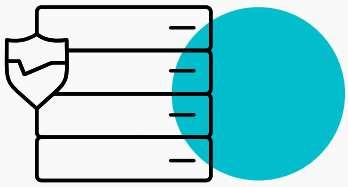
Access is permitted only to designated IT administrators, and from only specific IP addresses.

Survey Response Encryption

Especially when you are ensuring survey participants that their data is treated confidentially, it's critical for us to guarantee that responses are kept completely secure. SSL enables you to encrypt data during transmission, aiding in the secure transfer of confidential data.

Section 6

System Reliability



Data Backup and Frequency

Due to constant data updates, we perform daily, weekly, and monthly backups. Transaction and incremental backups are performed on a regular basis. On a monthly basis, a regular recovery testing plan is carried out to ensure backups and restoration processes run smoothly.

Documentation

Backup documentation regarding how system, application, and data backups are performed is reviewed every 3 months. Further reviews are completed whenever new hardware or applications are added.

System Uptime

We have an SLA of 99.9% uptime for our services.

Planned Maintenance

Planned downtime is limited to a maximum total of 8 hours per year, allowing for the performance of regular maintenance. All users are informed of the date and time of this maintenance at least one week prior.

Failover Configuration

We have failover in place for all critical hardware and software components, as well as for the entire site. An individual hardware mechanism is available as a failover for every component. We also have an offline failover system for complete failover in cold state when a daily backup copy is being restored.

Section 7

System Scans and Upkeep

Penetration Testing

We perform penetration system testing every six months and before every new release to eliminate any vulnerable areas in our network. Initial testing and fixes are carried out by internal personnel and are later audited by external sources.

Scans

We use Nessus, Nmap, and Zenmap third-party scanning tools. We also maintain an in-house security team.

System Patching

Important patches and updates are installed periodically on all of our systems. All servers are reviewed at regular intervals to make sure they are up to date. Before any patch is uploaded on production servers, it is uploaded on a local environment where a specialized team of QA testers verify and certify that uploading the patch will have no adverse effect on any of the applications, systems, or components. The patch management server monitors the need for any critical patches, which are uploaded within three days, following ample testing. Additionally, our Microsoft subscription provides us with advice about relevant patches and updates which we regularly review and implement as needed.

Section 8

Personnel Training and Access

Employee Screening

We perform background screening on all employees, to the extent possible within local laws.

Training

We provide all essential security and technology use training for all employees.

Administrative Access

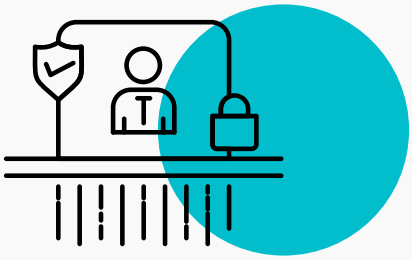
Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis.

Audit Logging

We regularly maintain and monitor audit logs on all our services and systems.

Service Providers

We screen our service providers and they are bound by contract to confidentiality and security obligations if they deal with any userdata.



Section 9

Development Practices

Coding Practices

Our engineers use the best coding practices and industry-standard secure guidelines which align with the OWASP Top 10. All development is done in-house and is never outsourced.

Deployment

We deploy code regularly to address any bugs identified on the production environment.

Section 10

Compliance and Certifications

EU-U.S. Privacy Shield

Sogolytics LLC. ("Sogolytics") participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework. Sogolytics is committed to subjecting all personal data received from European Union (EU) member countries, in reliance on the Privacy Shield Framework, to the Framework's applicable Principles. To learn more about the Privacy Shield Framework, visit the U.S. Department of Commerce's Privacy Shield List.

ISO 27001 Certified

Sogolytics is ISO 27001 certified, offering you the highest level of assurance in our business processes and practices. The rigorous ISO 27001 certification process includes an intensive audit by an accredited third party to certify that Sogolytics operates in a professional manner, values security highly, and complies with this internationally recognized top-tier standard. This certification also provides additional clarity regarding evaluation of the quality, breadth, and strength of our organization's security practices.

Data Center Certifications and Compliances

SSAE 16, SAS 70, SOC 2, PCI DSS and HIPAA compliances.

Swiss-US Privacy Shield Framework

We have failover in place for all critical hardware and software components, as well as for the entire site. An individual hardware mechanism is available as a failover for every component. We also have an offline failover system for complete failover in cold state when a daily backup copy is being restored.

Privacy Shield Framework

ISO 27001

BBB ACCREDITED BUSINESS

PRIVACY FEEDBACK Powered by TRUSTe

COMPLIANT HIPAA COMPLIANT

Section 11

In Case of a Security Breach

We have implemented extensive security measures to protect your Information. To access the system, a user must enter a unique User ID and password each time. The site is hosted in a secure server environment that uses a firewall and other technology to prevent access from outside intruders. Internally, we use security logs, train our employees, and limit access to only essential personnel. When transmitting sensitive Information, we use encryption technology. All our technology and processes are not, however, guarantees of security. If we do notice a security breach, we will notify the affected users via email so that they can take preventive actions.

Section 12

User Responsibilities

Sogolytics allows account administrators to create and manage sub-accounts and determine permission levels, eliminating risky password sharing, confusion and inefficiency, while maintaining data privacy. There will be times when sharing data with people inside and outside of your organization is essential to facilitating workflow; still, controlling access to sensitive information is the only way to ensure it is secure.

Prioritize security in your projects using enhanced security options and including or collecting only necessary participant data from your participants. Do not share your User ID or password. If you suspect that our security has been breached, email us immediately at privacy@sogolytics.com.

If you have any specific questions, please contact us at support1@sogolytics.com.

Email

support1@sogolytics.com

Phone

+1 (800) 646-0520