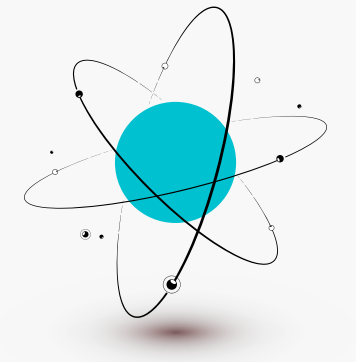
Sogolytics: Security at a Glance

- ISO/IEC 27001:2022 Certified
- PCI DSS v4.1 Compliant (SAQ A-EP)
- GDPR Compliant
- AES-256 Encryption
- SOC 2 Type II Audited Annually
- HIPAA & FERPA Aligned
- 99.9% Uptime SLA
- 24/7 Security Monitoring



Introduction

At Sogolytics, protecting the privacy, confidentiality, and availability of your data is one of our most important commitments. We recognize that security is not just a regulatory requirement but the foundation of customer trust.

From hosting in secure, industry-leading data centers to undergoing regular independent audits and certifications, we align with the strictest global standards, including ISO 27001:2022, SOC 2 Type II, PCI DSS v4.1 (SAQ A-EP), HIPAA, FERPA, and GDPR.

Our security practices extend beyond compliance. We continuously monitor threats around the clock, train our employees extensively, and embed security principles at every stage of system design, development, and operations.

Security Governance

Our security program is led by a dedicated security team reporting directly to executive leadership. We maintain a security steering committee that reviews policies, risk posture, and program effectiveness on a quarterly basis.

Annual risk assessments are conducted to identify, evaluate, and mitigate potential threats to our systems and customer data. Findings are tracked through remediation and reported to leadership until resolved.

Certifications and Compliance

We hold and maintain globally recognized certifications that validate our security program:

- **ISO/IEC 27001:2022 Certified** – Demonstrates adherence to international information security management standards.
- **SOC 2 Type II Audited Annually** – Confirms that our controls for security, availability, and confidentiality are designed and operating effectively.
- **PCI DSS v4.1 Compliant (SAQ A-EP)** – Ensures secure handling of payment card transactions.
- **GDPR, HIPAA, and FERPA Aligned** – Meets requirements for data protection, healthcare information security, and educational records privacy.

Data Security

Protecting your survey data is a top priority. We employ multiple layers of defense:

Encryption

- **Data in Transit:** All communications are encrypted using HTTPS with TLS 1.2 and TLS 1.3 protocols.
- **Data at Rest:** All customer data stored in our systems is encrypted using AES-256 encryption.
- **Key Management:** Encryption keys are managed using enterprise-grade key management systems with strict access controls and comprehensive auditing.

Infrastructure Protection

Our infrastructure employs next-generation firewalls, intrusion prevention systems, and web application firewall (WAF) technologies to defend against malicious traffic and common web exploits. Administrative access to systems is tightly controlled and monitored through secure, auditable remote access solutions. A centralized monitoring and alerting platform provides continuous visibility into system activity, enabling rapid detection and response to potential threats.

Physical Security

Sogolytics is hosted in secure, enterprise-grade data centers operated by leading cloud and colocation providers. These facilities maintain comprehensive physical security controls, including:

- 24/7 on-site security personnel and monitoring
- Biometric access controls and multi-zone security perimeters
- CCTV surveillance with extended retention
- Redundant power systems with UPS and generator backup
- Environmental controls including fire suppression and climate management
- SOC 2 and ISO 27001 certified facilities

User Security

Every user account is protected with a unique ID and password that are securely stored using industry-standard hashing algorithms. To strengthen authentication, multi-factor authentication (MFA) is available for all accounts. Sessions are managed with secure tokens that expire automatically, reducing the risk of unauthorized access.

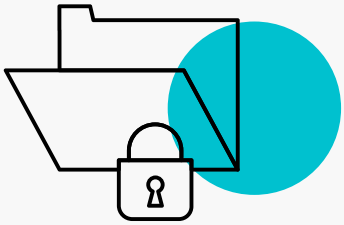
Customer Security Controls

Administrators have access to the following security features to protect their accounts:

- IP allowlisting to restrict account access to approved networks
- Custom password complexity requirements
- Password expiry
- Multi-factor authentication

Access to data is controlled through a role-based access model, ensuring users can only view or manage information appropriate to their responsibilities. We support Single Sign-On (SSO) integration with major identity providers, making authentication both seamless and secure. All access is logged and monitored, and anomalies are flagged for immediate review.

Privacy and Data Ownership



We maintain a comprehensive Privacy Policy that provides transparency on how data is collected, processed, retained, and shared. Key commitments include:

- **Full Data Ownership:** Customers retain complete ownership of their data and can export it at any time in multiple formats.
- **No Third-Party Sales:** Customer data is never sold to third parties.
- **AI/ML Training:** Customer data is not used for AI or machine learning training without explicit written consent.

Data Processing Agreement

A Data Processing Agreement (DPA) is available upon request for customers requiring documented contractual commitments under GDPR and other privacy regulations.

Data Retention

We maintain clear data retention policies to ensure customer data is handled appropriately throughout its lifecycle:

- **Active Account Data:** Retained for the duration of the subscription.
- **Closed Accounts:** When you close your account, your data is retained securely for a limited period to allow recovery, then permanently deleted.
- **Backups:** Retained for 6 months for security and compliance purposes.
- **Deletion Requests:** Processed within 30 days of verified request receipt.

Data Residency

All customer data is hosted in secure, geographically distributed data centers within the United States. These facilities are built with redundancy and resilience to ensure availability, and they undergo regular third-party audits to confirm compliance with globally recognized standards.

For international customers, we utilize Standard Contractual Clauses (SCCs) and other approved transfer mechanisms to ensure lawful cross-border data flows in compliance with GDPR and other applicable regulations.

Regulatory Compliance

Sogolytics complies with major international and U.S. data protection standards:

- **GDPR:** We support customer rights including access, correction, deletion, and portability of personal data.
- **HIPAA:** For healthcare customers, we maintain HIPAA-aligned safeguards to protect Protected Health Information (PHI).
- **FERPA:** For educational institutions, we comply with FERPA requirements, ensuring student records are secured and handled appropriately.

System Reliability

We understand that service availability is critical. Our systems are designed for resilience:

- **99.9% Uptime SLA** – Equivalent to less than 9 hours of unscheduled down-time annually.
- **Recovery Time Objective (RTO): 4 hours** – Maximum time to restore service after an incident.
- **Recovery Point Objective (RPO): 15 minutes** – Maximum data loss window in a disaster scenario.
- **Disaster Recovery:** Capabilities are built into our infrastructure with failovers across multiple geographic sites. Annual disaster recovery drills validate our preparednes.

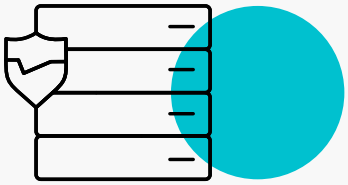
Business Continuity

We maintain a Business Continuity Plan (BCP) that is tested annually. Critical business functions can continue during disruptions through geographic distribution, redundant systems, and documented procedures. Our BCP addresses scenarios including natural disasters, infrastructure failures, and pandemic conditions.

Credit Card Security

Sogolytics does not store credit cards or payment details in its environment. All financial transactions are processed through a PCI DSS v4.1-certified payment processor. By ensuring that cardholder data never enters our core systems, we minimize risk and remain compliant with payment industry requirements.

Secure Development Practices



We follow a DevSecOps approach grounded in a secure software development lifecycle (SDLC), embedding security from design through deployment.

Code Security

Code is continuously reviewed and validated via automated and manual methods, including Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Software Composition Analysis (SCA) alongside unit and integration tests. Our coding practices align with OWASP Top 10 and ASVS guidelines.

Deployment Controls

All changes pass peer review and gated CI/CD controls including branch protections, signed builds, secrets scanning, and policy-as-code. We implement environment-specific approvals, progressive delivery, and rollback capability. Vulnerabilities are triaged with defined SLAs, and pipelines enforce fail-fast policies for critical findings before promotion to production.

System Scans and Upkeep

We operate a structured vulnerability management and patching program:

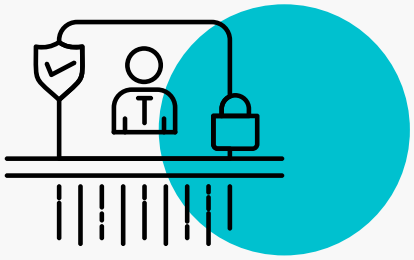
- Critical patches are tested and deployed promptly
- All systems are reviewed regularly to ensure they remain current
- Continuous vulnerability scanning across all environments
- Quarterly compliance scans
- Annual penetration tests through independent security firms
- Targeted testing before major releases

Personnel Security

Our people are a vital part of our security program:

- All employees undergo background checks
- Mandatory annual security training covering phishing awareness, data protection practices, and secure technology use
- Regular phishing simulations with consistent pass rates above industry benchmarks
- Employee access based on the principle of least privilege and reviewed regularly

Vendors and Service Providers



We carefully manage third-party risks:

- All service providers undergo security and compliance review before engagement
- Contractual obligations require providers to protect customer data
- Independent audit reports (SOC 2, PCI DSS) collected annually to validate controls
- Sub-processors include leading cloud hosting providers, secure payment processors, and trusted communication partners

Sub-processor List

A current list of sub-processors is available at https://www.sogolytics.com/subprocessor-list/ and is updated when changes occur.

Audit Logging and Monitoring

Sogolytics maintains a centralized logging and monitoring program to ensure visibility, accountability, and rapid detection of security events.

Security-relevant logs are collected from application components, infrastructure, authentication systems, and network controls and are centrally aggregated into a Security Information and Event Management (SIEM) platform.

Logs include authentication attempts, access to customer data, administrative actions, and system events. All logs are time-synchronized, protected from unauthorized modification, and retained in accordance with our log retention policy.

A dedicated 24×7 Security Operations Center (SOC) monitors security alerts and investigates anomalous activity. Confirmed incidents are handled in accordance with our documented Incident Response Plan, including containment, remediation, and post-incident review.

Incident Response and Breach Notification

We maintain a documented Incident Response Plan (IRP) and Breach Response Plan with clearly defined responsibilities and escalation paths. Our systems are monitored continuously to detect and contain threats quickly.

Notification Commitment

In the event of a confirmed security incident or breach involving personal data, we commit to notifying affected customers within 72 hours, consistent with GDPR and other applicable laws. Following an incident, we provide customers with a post-incident report detailing the impact, root cause, and remediation measures.

Security Breach Protocol

In case of a breach, our priority is immediate containment and mitigation. We initiate investigation procedures, preserve forensic evidence, and take corrective actions to restore services securely. Affected customers are notified promptly, and full transparency is maintained throughout the process.

Mobile Platform Security

On mobile platforms, we follow secure development practices, limit required permissions, and always request explicit user consent before collecting or processing sensitive data.

Insurance Coverage

Sogolytics maintains cyber liability insurance coverage to protect against data breach costs and service disruptions.

User Responsibilities

While we provide strong technical and organizational safeguards, customers also play an important role in maintaining security:

- Enable multi-factor authentication (MFA) for all administrator accounts
- Assign access based on the principle of least privilege
- Protect account credentials and never share passwords
- Report any suspicious activity immediately to privacy@sogolytics.com

sogolytics

Contact Us

For security and privacy inquiries:
privacy@sogolytics.com.

Disclaimer: This document provides an overview of Sogolytics' security posture. It is intended for informational purposes only and is not exhaustive. Feature availability may vary by plan; please refer to your service agreement for contractual details.