SurveyGizmo Security Overview

GDPR Compliance

Visit SurveyGizmo's GDPR Command Center for the latest information.

Table of Contents

Information Security - Executive Summary

At SurveyGizmo we take security very seriously.

SurveyGizmo is a globally utilized application. As such, we strive to ensure compliance with specific requirements; but we do not guarantee it. We have implemented a holistic and comprehensive approach to both security and privacy, but SurveyGizmo does not claim to have a complete understanding of all the

unique compliance and privacy requirements of each country.

We provide you with the tools, but it is up to you to implement these tools correctly. Ultimately, the security of the data that you collect using SurveyGizmo, is your responsibility.

> **Use of Data**: Customer acknowledges and agrees that SurveyGizmo may analyze Customer's content and usage of the Services to derive aggregated, anonymous statistical data regarding use of the Services ("Analyzed Data"). SurveyGizmo may combine and incorporate such Aggregated Data with or into other similar data and information regarding use of the Services. Under no circumstances will Aggregated Data (i) include any data provided by respondents to a survey, or (ii) identify Customer, its users or any survey respondent.

Our executive management has approved all Information Security and Privacy policies. We annually review all our Security and Privacy policies, and this document will be updated to bring you the most current information about our data protection efforts. Our Application Security and Compliance Manager is responsible for compliance and security at the team level.

> SurveyGizmo does not allow unauthorized, external parties to conduct testing against our systems.

> **What will happen to a customer's data upon termination of the contract?**
> A written request to permanently remove all response data from a survey must be submitted by a customer. Per written request, SurveyGizmo may provide written confirmation that all files, database records, and backups of data have been destroyed. Data cannot be recovered after execution. Data always remains the property of the customer and written requests to destroy data may be submitted at any time.

Artifacts

SurveyGizmo Information Security Overview

Download SurveyGizmo Information Security Overview PDF

Cloud Security Alliance Consensus Assessment Initiative Questionnaire (CSA CAIQ)

Download CSA CAIQ PDF

Standardized Information Gathering (SIG) Questionnaire

Download SIG Questionnaire PDF

Third-Party Penetration Test Executive Summary

Download Third Party Penetration Test Executive Summary PDF

WhiteHat Security Testing Executive Summary Report

ExecutiveSummaryReport_20200318-091111_64791.pdf

Payment Card Industry Data Security Standards (PCI-DSS) Certificate of Compliance

trustwave_compliance_certificate 2.pdf

SurveyGizmo Third-Party Vendors

A comprehensive list of all of SurveyGizmo's third-party vendors and services that SurveyGizmo uses to provide support/service to our customers. While all vendors listed do not meet the GDPR definition of a sub-processor, we are electing to be fully transparent regarding all relationships.

Download SurveyGizmo Third-Party Vendor List PDF

System Configuration

SurveyGizmo is located in Boulder, Colorado. We utilize Amazon Web Services (AWS) for our hosting services.

SurveyGizmo has separate development, test, and production environments for both our website and application. Work progresses from development to quality assurance to production, where it can be seen and used by our customers.

A modified Lean Agile System Development Life Cycle (SDLC) methodology is used for development. Issues are reported by both clients and employees. Issues are tested and documented in Support and prioritized by the Product Development Team.

To ensure a secure platform, we utilize the Open Web Application Security Project (OWASP) standards during the software development process. We focus on not only improving the functionality of our product but also improving the security of our software. For more information, please see OWASP top 10.

We use a code repository along with a managed ticketing, review, and approval process. Our development team utilizes standard quality assurance procedures, and automated regression testing is performed prior to each production deployment.

We also never outsource; all development and quality assurance activities are performed in-house.

We never use production data for testing purposes, unless it is required to resolve a client-reported support issue.

Robust monitoring software is used to monitor performance and to notify us of any problems in our production environment. The checks include, but are not limited to, business logic, database layer, disk space, resources, and application logs.

Third-Party Architecture

Because we are hosted by AWS, we leverage their power to be highly available, to increase our reliability, and to offer increased flexibility that lets us scale up for surges in traffic in almost real-time.

Automated redundancies are in place for a scalable infrastructure to accommodate high traffic. Because of this, security in the cloud is slightly different than security in on-premise data centers. We have a shared

security responsibility model with AWS. We utilize AWS for infrastructure as a service (laas), and they are responsible for the underlying infrastructure that supports the cloud. They are also responsible for protecting the global infrastructure that runs all of the services offered in the AWS cloud. This infrastructure is comprised of the hardware, software, networking, and facilities that run AWS services. For more information regarding Amazon's extensive security controls, see their Overview of Security Processes Whitepaper.

For security reasons and as part of AWS policy, AWS does not provide the physical addresses of the data centers. The main reason our customers would want the physical address is to ensure the data centers are sufficiently geographically separated to conform to standard disaster recovery requirements. AWS ensures they have that level of redundancy and reliability, which eliminates the need for actual physical addresses.

All network components are configured in a redundant fashion. All customer data is stored on a primary database server with multiple active clusters for redundancy. The database servers utilize RAID disks and multiple data paths to ensure reliability and performance.

Endpoint Management

We use industry-standard endpoint protection software on all company laptops and they are regularly patched. Laptop scanning is scheduled to run daily, and employees are encouraged to report any errors to the privileged IT Admins. We manage administrator privileges on all equipment and all new laptops are encrypted.

Access Control, Identification, and Authentication

Individual accounts are provisioned for each employee and either password or MFA, depending on the system, is utilized to authenticate their access. Once an employee leaves, the account is terminated the same business day. Accounts are reviewed annually to ensure continued business need and validity.

Application Scalability & Redundancy

In order to ensure that data collected for different purposes can be processed separately, SurveyGizmo logically separates the data of each of its clients. We ensure that each customer has a unique login ID and that data segmentation is keyed off a unique customer ID. Each customer has a unique username (email address) and a unique password.

After repeated, unsuccessful logins, the lockout features prevent the login page from being resubmitted. We are also able to scale horizontally to support increasing users and customers.

We leverage a number of queuing systems to defer jobs that do not need to be transactional. This allows us to scale up and down the number of queues and workers to mirror the demands on our systems without impacting the front-end experience of users in the application.

To ensure that we never lose any of our customers' data, we have multiple strategies utilizing redundant data stores. This includes RAID-based storage and Master / Read Databases in-memory caching.

Data Encryption

We encrypt data in transit, at rest, and on all backups.

Here's how: Access to the SurveyGizmo Application is available only through secure HTTPS. Data in transit is encrypted when customers choose to use HTTPS protocols for their account. We utilize TLS for our secure communication protocol and we are currently at the most recent patch level.

All survey data, even for those that are designated as unencrypted, is encrypted at the disk level - "at rest". Amazon Simple Storage Service (Amazon S3), provides SurveyGizmo with secure, durable, highly-scalable cloud storage which is designed to deliver 99.999999999% durability - yeah that is ***eleven*** 9s!! Surveys that are designated by the customer as encrypted by way of the Project Data Encryption feature, are further encrypted at the row level in the database. Once you have collected data in an encrypted survey, encryption cannot be enabled/disabled.

In addition to this, your data is backed up using Amazon Elastic Block Store (EBS) snapshots which is used as a primary storage device for data that requires frequent and granular updates. Automated encrypted snapshots (differentials) of databases are performed daily, and all data storage is redundant.

Our redundant databases reside in a private subnet that is only accessible via our application and web servers. Additionally, we leverage Amazon's AWS security features to further "lock down" access to these systems. Bulk response data can only be accessed via the reporting and exporting features available via the application by a customer logging in with their credentials over https.

Scanning and Patching

Unlike other SaaS vendors that you may be working with, we have contracted with an independent third party to not only do a point-in-time penetration and business logic test but also to perform a continuous scan of the application so we ALWAYS have an independent third party looking at our application. **These reports are available at our highest plan level only**.

Production servers are frequently patched to ensure their security is always up to date. We roll patches out through the development rollout process - development to QA to production. We mitigate all vulnerabilities within our predefined timeframes.

Logging and Alerting

Firewall logs and other logs are restricted to authorized users via secure multi-factor authentication (MFA) controls. We utilize Amazon's Recommended MFA, and only our privileged IT Admins have access to this information.

We utilize intrusion detection (IDS) and Intrusion Prevention (IPS) at multiple layers of the application, with extensive logging and alerting capabilities. We monitor criteria for thousands of different alerts ranging from customer experience and application health to server and service metrics.

Disaster Recovery Plan

We have a disaster recovery plan that includes shared responsibilities with Amazon and it is reviewed annually. Amazon utilizes disaster recovery facilities that are geographically remote from their primary data center. When using the AWS disaster recovery shared security model, they provide the physical infrastructure, network, and operating systems, and SurveyGizmo ensures the proper configuration and

logical access to the resources.

Business Continuity Plan

Our employees are trained annually on the Business Continuity Plan during the tabletop exercise. We have identified the critical business functions to ensure our uptime commitment. Our BCP includes the following phases: activation and notification, recovery, reconstitution, and lessons learned.

Incident Response Plan

Incident Response is a significant aspect of any Information Technology program. Preventive activities such as application scanning, password management, intrusion detection and intrusion prevention systems, firewalls, risk assessments, malware & anti-virus prevention, and user awareness and training can reduce the number of incidents. However, not all incidents can be prevented.

Our plan covers the Incident Response Requirements, Roles and Responsibilities of each Incident Response Team member, their contact information, Incident Handling Procedures, Incident Reporting Procedures, and complementary Metrics.

We have procedures for normal business hours as well as for after-hours and weekends. All employees are trained in the procedures, and they understand how and when to escalate an issue.

Our Compliance Manager and the IT Manager are responsible for enforcing information security policies, procedures, and control techniques to address all applicable requirements. They also ensure 100% participation of personnel in the Security Awareness Training Program.

Breach Notification

Suspected incidents are reported to the Team Managers, who are responsible for organizing the investigation and notifying internal stakeholders. If the investigation finds a need for containment, that will occur, and then analysis will follow. If repair, recovery, or remediation is needed, that will follow.

Notifications to clients will be made based on contractual or legal obligations, reporting will be made to Executive Management, and training issues will be addressed. If a breach is detected with your data, you will be notified as soon as we are able to notify.

Security Skills Assessment and Appropriate Training

Policies

All employees are required to sign industry standard policies included but not limited to Non-disclosure Agreement (NDA), Acceptable Use Policy, and Work from Home (WFH) Policy.

All employees are issued company-owned equipment, and all company-owned equipment is managed by the office IT administrators. Per company policy, employees cannot access customer data from their personal devices, including laptops and cellphones.

We partner with an employment screening vendor to complete background checks on all employees before they are hired. The human resources department completes reference checks on all employees. We

comply with the federally mandated requirements regarding I-9 (The Employment Eligibility Verification Form) documentation.

Training

We have developed a robust, ongoing training plan for all new and existing employees. All new employees are required to attend SurveyGizmo training which includes an hour and a half of security training.

Existing employees receive annual refresher Security Awareness Training. We have a weekly company meeting where the Executive Management Team reports our revenue, expenses, and account numbers. We also utilize this time with the entire company to discuss important topics, like security and compliance training.

In 2016, we implemented user behavior training during which we 'phish' our own employees. This training allows us to train our employees on good email and web browsing habits.

SurveyGizmo Security White Paper

Download

Related Articles