At SurveyGizmo, we take security and data protection and privacy very seriously. Our goal in this whitepaper is to address general questions regarding international privacy concerns so you can conduct survey projects with confidence.

First, a disclaimer: this paper is not legal advice and should not be relied on as legal advice. SurveyGizmo strongly encourages its customers to ensure they have done their due diligence regarding whether or not they can entrust a third party with the data that they intend to store with us. If you know you have specific requirements your company must meet, you are accountable for understanding and implementing them; the requirements apply to you. SurveyGizmo can assist you, but we can’t ensure you are compliant. Ultimately, it is your data and you are responsible for it.

Security Questions: General and Specific

Because SurveyGizmo is primarily a Do-it-Yourself (DIY) application and is utilized globally, this whitepaper does not attempt to address unique privacy policies or specific government acts/laws for each country. Rather, it provides general guidelines for how SurveyGizmo addresses privacy concerns.

We strive to ensure compliance with specific requirements, but we don’t guarantee them. 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 requirements for each country.

In this paper, we will explain how we utilize your data, but specific compliance with each unique and specific regulation is ultimately the customer’s responsibility.

Speaking generally, all SurveyGizmo data is protected by numerous anti-hacking measures, redundant firewalls, and constant security scans. These protections cover account information as well as data collected within surveys.
But questions typically arise concerning the implementation of a unique privacy policy or specific government act or law, and how these might impact someone’s use of SurveyGizmo’s services when they store and process data containing personal information.

Data storage presents all companies, cloud-based and on premise, with many challenges, including:

- Will the data be secure?
- Where will the data be stored?
- Who will have access to the data?
- What laws and regulations apply to the data?
- What is needed to ensure compliance?

These considerations are not new, and they are not specific to Software-as-a-Service (SaaS). They are relevant to all instances of data collection. When using SurveyGizmo, each customer maintains complete ownership and control of their data. SurveyGizmo provides our customers with tools to assist them in the management of data, but control of the data, access to the data, and proper implementation of SurveyGizmo tools is always up to the customer.

Amazon Web Services and SurveyGizmo

SurveyGizmo utilizes Amazon Web Services (AWS) for its data hosting and storage services. AWS datacenters are built in clusters in various global zones. These clusters are referred to as AWS regions. AWS has obtained approval from the EU data protection authorities, known as the Article 29 Working Party, for the use of AWS Data Processing Addendum and Model Clauses.

Because of this, AWS customers, whether established in Europe, Canada, Australia or any global company with operations in the European Economic Area, can continue to run their operations using AWS in full compliance with the EU Directive. For more information, please see Amazon's compliance resources.
SurveyGizmo does not transfer data between the EU datacenter and the US datacenter. If a customer wishes to store data in both the US and in the EU, SurveyGizmo requires them to have a unique account in each datacenter and this data is not commingled.

**How we handle data:**

**Customer Data:** When you register on our website, we ask for your name and contact information, including: company name, name of contact, title of contact, company address, telephone number, email address, username and password, and billing information, which may include credit card numbers. We don’t store any credit card information; instead, we use a third party service as a credit card processor.

**Respondent Data:** As a data collection tool, we receive respondent information from survey respondents. If you are using our email campaign distribution method, you provide us with the email address, and optionally other contact information, of each respondent.

Before receiving that information, we contractually require that you warranty that you have a pre-existing relationship with the survey respondent and/or the survey respondent's permission to receive electronic messages.

Permission is considered to be granted when a contact has asked to be subscribed to a list and an email is sent to confirm the validity of the email. This "double opt-in" process ensures that all contacts have been given permission to receive bulk email, and that they have provided a valid email address that will not result in bounced messages or SPAM abuse reports.

**EU Data:** All EU data collected in SurveyGizmo is stored in the Germany datacenter; data is never stored outside the EU. We have staff in the United States, who at your request, can take actions to assist you with questions regarding your data. Before the end of 2016, it is SurveyGizmo’s intention to have staff in London and they will handle all data related issues - making Model Clauses unnecessary. As a general rule, we do not sign Data Processing Agreements (DPA) or Model Clauses. If you feel you need this level of protection, please contact your account manager and they can work through the details with you.
Customer Tracking and Data Collection

We utilize the following tracking technologies and services:

- Cookies
- Clear Gifs (Web Beacons/Web Bugs)
- Integrations
- Blogs/Forums
- Community Pages

All of our staff is located in Boulder, Colorado, USA. We will only access your data at a minimum necessary standard in order to provide technical or administrative support.

For instance, if you open a support ticket, hire our programming services, or your account is flagged for a security reason, then our staff may log into your account for the purpose of troubleshooting and correcting the reported issue or performing their contracted task. We will not for any reason disseminate your data other than as you have directed (e.g. email actions, sending reports, etc.). All your data is subject to the confidentiality clause (Section 11) of our Terms of Service.

Survey Data and Government Agencies

SurveyGizmo frequently gets questions about the rights of domestic and foreign government agencies to access data held in cloud services. Customers are often confused about issues of data sovereignty, including whether and in what circumstances governments may have access to their data.

The local laws that apply in the jurisdiction where the data is located are an important consideration for some customers. However, customers also need to consider whether laws in other jurisdictions may apply to them. Customers should seek legal advice to understand the application of relevant laws to their business and operations.

When concerns or questions are raised about the rights of domestic or foreign governments to seek access to data stored in the cloud, it is important to understand that relevant government bodies may have rights to issue requests for such data under laws that already apply to the customer.
For example, a company doing business in Country X could be subject to a legal request for information even if the data is stored in Country Y. Typically, a government agency seeking access to data from one of our customers will address any request for information directly to that entity, rather than to SurveyGizmo.

Under limited circumstances, SurveyGizmo could be asked to release your information to a government agency. If SurveyGizmo is subpoenaed to release your information, we would comply with the law. If we are legally able to notify you in advance, we will do so. SurveyGizmo has never been subpoenaed nor been involved with a data breach or significant privacy issue.

**Incident Responses**

SurveyGizmo has an Incident Response Plan, and data breach notification is part of this plan. SurveyGizmo will notify you regarding any loss, illegal transmission, or third party acquisition of data, regardless of the reason.

Notifications will be made by SurveyGizmo to you no later than 32 business hours after SurveyGizmo has become aware of an event, unless the notification would impede the necessary investigation. SurveyGizmo shall take appropriate measures and consult with you regarding the breach of security concern your data, as well as the reduction of potential damages to the data subjects.

Insofar as notification obligations apply to the data subjects, SurveyGizmo will assist you in fulfilling these obligations.

We are always investigating new developments in the privacy and data protection realm. As we are constantly improving our services and expanding our business, we reserve the right to modify this information at any time. All information is subject to our [Terms of Service](mailto:Compliance@surveygizmo.com).}

Our team strives to ensure accurate information, but because we are always evolving our security posture to match current and changing conditions, this document may not always be error free. For questions or comments please contact [Compliance@surveygizmo.com](mailto:Compliance@surveygizmo.com).
This document was created with the following references. In some cases, complete sections were used from Amazon resources:

https://aws.amazon.com/compliance/resources/
https://aws.amazon.com/security/
https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf
https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf