Overview of SnapApp and Data Privacy

Last Updated December 1, 2018

1. SnapApp overview

The SnapApp interactive content marketing platform provides marketers the power to create, publish, promote and measure engaging interactive content experiences as part of their demand generation and customer marketing initiatives (each such experience is a separate "App"). SnapApp is a multi-tenant SaaS solution, which customers use in self-serve or managed-services mode to build content to their specification. SnapApp does not provide custom software development or custom agency/professional services to customers.

2. Data collection via the SnapApp Platform

Customers configure their Apps to collect end user data (through both in-experience questions and lead forms) and securely deliver that data to their marketing automation platform through either APIs or web-forms, provided by each marketing automation provider. Customers determine what data is collected through their Apps, subject to the prohibition on collecting Sensitive Information (such as financial, health, government, or employment information) as defined by Section 3.3 of SnapApp's Platform Terms of Service.

All such data collected passes through SnapApp's servers and as such SnapApp is deemed the processor of such data with the Customer remaining the Controller of said data. Under the Terms of Service, SnapApp is prohibited from using any of the PII collected, which remains the property of the Customer at all times. Since Customers are considered the Controller of the data collected through their Apps, all such data is subject to each Customer's specific Privacy Policy.

SnapApp's Privacy Policy governs only with regard to the data we collect from our Customer's and their employees through their use of the SnapApp platform.

3. Platform infrastructure

SnapApp is a multi-tenant web hosted solution that enables customers to build and host the Apps they create on the SnapApp platform and then use embed code to serve the content to targeted end users from a variety of web sources including CMS landing pages, social media platforms, and responsive mobile web pages. Apps are served as javascript within an iframe.

SnapApp production applications and services are entirely hosted in an Amazon Web Services (AWS) environment, creating a shared responsibility security model with AWS. AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. In turn, SnapApp assumes responsibility and management of the guest operating system (including updates and security patches), application software, and the configuration of the AWS-provided firewall support.

The specifics regarding SnapApp's approach to data privacy and security are documented in the SnapApp Security Systems and Procedures document, which is available upon request. Information regarding AWS's approach to data privacy and protection can be found here.

4. Data Retention Approach

Any data collected through the platform by Customers is stored actively in the SnapApp production environment for the agreed Data Retention Period (1- 30 days), based on Customer discretion. By default the data is configured to be pushed in real-time to the Customer's marketing automation platform through either APIs or web-forms, provided by each marketing automation provider. Alternatively, Customer's may instruct SnapApp in writing to provide access to enable secure download of the data directly from the SnapApp platform. At the end of the agreed Data Retention period all collected data is deleted.

5. Commitment to Data Protection – GDPR and Privacy Shield Certification

The technical and process measures that SnapApp has implemented regarding data security, as described in the SnapApp Security Systems and Procedures document, have been designed to ensure we are supporting our customers who are subject to GDPR, where SnapApp is considered the processor of data collected through its platform. SnapApp has had its GDPR Privacy Practices Compliance validated by Truste and a summary of findings can be downloaded here.

SnapApp's continued certification under the EU-US and the Swiss-US Privacy Shield framework is considered to allow our customers to fulfil their obligations regarding the transfer of personal data to recipients outside the European Union. The Truste Certified privacy seal is displayed on the SnapApp.com web site and details about SnapApp's EU-US and Swiss-US Privacy Shield certification are available on the official Privacy Shield website here.

SnapApp will enter into an appropriate Data Processing Agreement (DPA) as required under GDPR regulations and can provide a standard form DPA or review a customer's preferred form. SnapApp's standard DPA can be downloaded here.