



APPTROVE

12 JULY 2024

A Self Attestation Report on
Controls Relevant to CCPA



Self Attestation by



Akitra Inc.
830 Stewart Dr Suite 269, Sunnyvale,
CA 94085, United States

Table of Contents

- Section 1: Organization information
- Section 2: Audit information
- Section 3: System Description
- Section 4: Audit Objective
- Section 5: Scope
- Section 6: Internal Auditor's Report
- Section 7: Audit Details

➤ Section 1: Organization information

Company name:	Apptrove
Contract Person:	Srishti Sharma
Main address:	B1/H3 Ground Floor Mathura Road Mohan Cooperative Ind. Area Badarpur, New Delhi, Delhi - 110044
Address of other sites:	2035 Sunset Lake Road, Suite B-2, Newark New Castle County, Delaware 19702
Phone number:	+91-9355019797
Website:	https://apptrove.com/
Total number of employees:	35
Total number of employees within the scope:	35
Contact name:	
Contact email:	
Contact phone:	

➤ Section 2: Audit information

Audit standard(s):	CCPA	
Audit type:	Internal Audit	
Date(s) of audit(s):	12 JULY 24	
Duration:	Point in time audit.	
Site(s) audited:		

Audit team:	Akitra Internal Audit Team
Additional attendees and roles:	

➤ Section 3: System Description

INSTRUCTIONS:

AICPA Requirements: “A SOC 2® examination is predicated on the concept that, because service organization management is ultimately responsible for developing, implementing, and operating the service organization’s system, service organization management is also responsible for developing and presenting in the SOC 2® report a description of the service organization’s system”- AICPA

Source: <https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/dc-200.pdf>

DC 1: Company overview and types of products and services provided

Approve is a mobile marketing platform that helps you track all the statistics of your application along with a dashboard for all the affiliate management practises.

With a pack of features like unilink, fraud detection, reporting, audience creation and integration - Approve offers it’s users the ability to track all the campaigns and partner and agency activities

DC 2: The principal service commitments and system requirements

Our terms of service - <https://apptrove.com/terms-of-service/>

Privacy policy - <https://apptrove.com/privacy-policy/>

Our billing policy -

<https://apptrove.com/billing-policy/>

Our SLAs

Working hours

- Indian Client - Mon - Fri - 11 am to 8 pm
- US & Europe Client - Mon - Fri - 11 am to 11pm

Leave

- Inform the POCs 1 day before your leave
- Notify on the respective groups
- Update calendar meetings

Meeting Guidelines

- All the meetings should be booked on the Google calendar and should have a Fireflies recording attached to it (Post-ending of the call)
- After every call, a meeting summary should be posted on primary channels and an email should be drafted and sent within 3 working hours.
- In case you have been invited for a meeting, accept or decline the invite within 1 hour of that received invitation.
- In case you decline, mention the appropriate reason for it such as conflicting with another call etc.

Query from Client - End

- Acknowledge the query as soon as you encounter it
- Respond to the query
 - a) Within 30 minutes if not in a meeting or call
 - b) Within 60 mins if in a meeting or on a non-working day from 11 am to 7 pm
- Indian Client - If the client has a query at night or after 8 pm then the next reply or acknowledgement should be the next day before 11 am
- US or Europe Client - If the client has a query at night or after 11 pm then the next reply or acknowledgment should be the next day before 11 am
- Basic query resolution within 2 working hours

In case of a bug - Share the status within 3 hours once resolved or unresolved

Feature Requests

Give an ETA for the feature building post consulting with the product team, and acknowledge the request message within 3 hours

DC 3: The components of the system used to provide the services

3.1 Primary Infrastructure and Applications:

Application/System	Process/Transactions	Purchased or Developed	Platform and Operating System	Database	Data Type
Custom HR System	Employee records and HR processes	Purchased		Zoho People	Employee information
Finance System	Payroll data	Purchased		Zoho Payroll	Employee's payroll
Tech Team	Version Controlling	Purchased		Github	Code hosting and sharing
Tech team	Build, test, and deploy their software.	Purchased		Jenkins	Code Build
Billing Software	Customer's billing	Developed			To manage customer's billing and invoice

3.3 People:

Apptrove has a staff of 35 employees and contractors.

3.4 Security Processes and Procedures:

Privacy policy - <https://apptrove.com/privacy-policy/>

3.5 Data:

Customer's personal data - Apptrove do not track or store any customer's personal data without the consent from the client. The data is not passed along to any third-party tool and is stored as part of our databases with all necessary safety measures

Login Password: The registration requires you to create a password for accessing of Apptrove services, which is confidential and sensitive information, collected and retained within Apptrove database. But the said sensitive information is just used by you as a Apptrove user for gaining access to the services and is not used or accessed by Apptrove or its affiliates/partners in any way.

Financial Information: The Bank Details may be visible on the cheques couriered to us for payment of any services, but the complete bank account details are never noted down or processed for any reasons whatsoever, with us. Though we recommend direct deposit of payments in our Bank Account either electronic transfer or by the drop of a cheque.

3.6 Third Party Access:
Already given

3.7 System Boundaries: (Product lines/ LOBs/ brands)

Product list -

Apptrove uses advanced technology and a customer-first approach to help marketers across the globe build great products, create exceptional experiences, and preserve customer privacy.

Apptrove - Mobile measurement platform - Tracks your app growth and creates a platform for you wherein you can integrate with different sets of partners and view results of the same.

DC 4: Disclosures about identified security incidents

Not received any such incident or notification for any major failure.

DC 5: The applicable trust services criteria and the related controls designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved

Background Check Process (BC1)

The background verification checks on Apptrove personnel are conducted in compliance with relevant laws and regulations and are tailored to the business needs, the classification of information accessed, and the associated risks. These checks include criminal history screenings unless restricted by local laws. Additionally, all third parties with technical, privileged, or administrative access to Apptrove production systems or networks must undergo a background check or provide evidence of an acceptable background, reflecting their level of access and the perceived risk to Apptrove. The background check process, managed by Chekr, includes automated checks complemented by manual reviews.

Background Check Process (BC2)

The background verification checks on Apptrove personnel are conducted in compliance with relevant laws and regulations and are tailored to the business needs, the classification of information accessed, and the associated risks. These checks include criminal history screenings unless restricted by local laws. Additionally, all third parties with technical, privileged, or administrative access to Apptrove's production systems or networks must undergo a background check or provide evidence of an acceptable background, reflecting their level of access and the perceived risk to Apptrove. The background check process includes both automated checks and manual reviews.

DC 6: Complementary User Entity Controls (CUECs):

Apptrove's services are designed with the assumption that certain controls will be

implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Apptrove’s services to be solely achieved by Apptrove’s control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Apptrove.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities’ locations, user entities’ auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

Trust Services Criteria	Complementary User Entity Controls
CC2.1	User entities are responsible for the security and integrity of data housed under user entity control, particularly the data utilized by Organization systems and services.
CC6.2	Determination of personnel who need specific functionality and the granting of such functionality is the responsibility of authorized personnel at the user entity. This includes allowing access to Organization’s application keys and API keys for access to the web service API
CC6.3	Authorized users and their associated access are reviewed periodically
CC6.6	User entities will ensure protective measures are in place for their data as it traverses from user entity to Organization.
CC6.6	User entities should establish adequate physical security and environmental controls of all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity in order to provide authorized information to the Organization.

DC 7: Complementary Subservice Organization Controls (CSOCs):

Although the subservice organization has been “carved out” for the purposes of this report, certain Trust Services Criteria are intended to be met by controls at the

subservice organization. Complementary Subservice Organization Controls (CSOCs) are expected to be in place at GCP related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities. Management of Apptrove receives and reviews the GCP SOC 2 report annually. In addition, through its operational activities Apptrove’s management monitors the services performed by GCP to determine whether operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also has communication with the subservice organization to monitor compliance with the service agreement, stay abreast of changes planned at the hosting facility, and relay any issues or concerns to AWS/Google/Azure management.

It is not feasible for the criteria related to the System to be achieved solely by Apptrove. Therefore, each user entity’s internal control must be evaluated in conjunction with Apptrove’s controls and related tests, and results described in Section 4 of this report, considering the related CSOCs expected to be implemented at the subservice organization as described below.

Criteria	Complementary Subservice Organization Controls
CC6.4	GCP is responsible for restricting data center access to authorized personnel.
CC6.4	GCP is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC7.2	GCP is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
CC7.2	GCP is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
CC7.2	GCP is responsible for overseeing the regular maintenance of environmental protections at data centers.

DC 8: Disclosures of significant changes in last 1 year

- None made

➤ Section 4: Audit Objective

This self-attestation serves to affirm that Apptrove has implemented the necessary measures and practices to comply with CCPA. The objective is to provide transparency regarding our data protection efforts and to demonstrate our dedication to safeguarding personal data in accordance with regulatory requirements.

➤ Section 5: Scope

The audit process involved a comprehensive review of the following areas:

- **Data Collection and Usage:** Assessment of practices related to data collection, processing, and usage to ensure compliance with CCPA requirements.
- **Consumer Rights:** Examination of mechanisms for consumers to exercise their rights under the CCPA, including the right to access, delete, and opt-out of data sale.
- **Data Security:** Evaluation of the security measures in place to protect consumer data from unauthorized access or breaches.
- **Training and Awareness:** Review of employee training programs and awareness initiatives regarding CCPA compliance and data protection.

➤ Section 6: Internal Auditor's Report

To: Apptrove

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls based on our examination. The examination was conducted by Akitra. The following document provides a detailed account of your CCPA compliance efforts. We have approached this self-attestation with rigor and transparency. An examination of the service organization's the suitability of the design and operating effectiveness of controls involves:

- Obtaining an understanding of the service organization's service commitments and system requirements.
- Assessing the risks that the controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the controls are implanted as per standard criteria.
- Testing the operating effectiveness of controls stated in the Audit Report to provide reasonable assurance that the service organization achieved its service commitments and system requirements
- Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

➤ Section 7: Audit Details

CTL ID	Control Description	Findings	Compliance Status	Remark
CTL12275	Appropriate technical and organizational measures have been implemented by the organization for the security and protection of personal information. These measures are assessed by management on an annual basis and deficiencies identified are remediated in a timely manner.	Encryption Policy, Proof of encryption at Rest or Transit, Security Review Meeting Minutes	Compliant	
CTL12273	Requests received from controllers regarding exercising rights of data subjects are documented, retained, and acted upon without undue days.	Data Privacy Policy	Compliant	
CTL12270	The organization responds promptly to data subjects' requests to modify or withdraw their consent at any time. Records of such requests are documented and retained in accordance with organizational policies.	Data Privacy Policy Data Retention Policy Employee Training Status Report	Compliant	
CTL12271	The organization has established a privacy notice for its employees and contractors which specifies their rights and the organization's privacy obligations in accordance with applicable privacy laws and regulations. The policy has been communicated and	Data Privacy Policy, Employee Privacy Policy and Notice (Latest), Employee Training Policy, Employee Training Status Report, Human Resource Security Policy	Compliant	

	acknowledged by the employees and contractors on at least an annual basis or during significant changes.			
CTL12268	The organization retains personal information consistent with its privacy commitments and as long as it is required for its intended purpose.	Data Retention Policy Privacy Policy	Compliant	
CTL12274	Data Protection policy is established and communicated to employees and contractors within the organization. The policy is reviewed by management on an annual basis or in case of significant changes.	Data Privacy Policy Employee Training Policy Employee Training Status Report Human Resource Security Policy Policy Review Note	Compliant	
CTL12272	Organization has a privacy policy published on its website which outlines privacy obligations and specifies data subject rights in accordance with applicable laws and regulations. The policy is reviewed by management on an annual basis.	Employee Privacy Policy and Notice (Latest) Employee Training Status Report Policy Review Note Privacy policy published on the website	Compliant	
CTL12269	Explicit consent is obtained and maintained from data subjects prior to collection and for any new uses or disclosure of their personal information. Data subjects are provided with a mechanism to modify or withdraw their consent.	1. Cookies Accept 2. Data Privacy Policy 3. Privacy Acknowledgement 4. Privacy policy published on the website 5. Terms acknowledgement	Compliant	

CTL12267	<p>Employees and contractors are required to complete an information security and privacy awareness training as part of the onboarding process and annually thereafter.</p>	<p>Employee Training Policy Employee Training Status Report Human Resource Security Policy</p>	Compliant	
CTL12276	<p>Organization has designated a representative in the European Union to represent the organization regarding their obligations under the GDPR and to deal with any supervisory authorities or data subjects.</p>	<p>Data Privacy Policy Job Description - DPO Roles Policy</p>	Compliant	
CTL12278	<p>Organization maintains written contract with controllers on behalf of whom it performs processing of personal data. These contracts outline the security and privacy requirements that are required to be implemented by processors for the protection of personal data.</p>	<p>Risk Assessment Report Vendor Agreement Template Vendor Management Policy Vendor Risk Assessment Report</p>	Compliant	
CTL12279	<p>Organization maintains a record of processing activities with respect to personal data collected from data subjects or processed on behalf of the controller. The documented inventory is reviewed by management on at least an annual basis and provided to legal authorities on request.</p>	<p>Security Review Meeting Minutes DATA CLASSIFICATION POLICY</p>	Compliant	

CTL12280	Data breach risk assessment is performed on the identified incidents following the discovery of a breach to determine the probability that personal data has been compromised and whether notifications are required.	Business Continuity and Disaster Recovery Policy Policy Review Note Risk Assessment Policy Risk Assessment Report Table Top Exercise	Compliant	
CTL12281	Notifications are provided to controller(s) regarding personal data breaches without unreasonable delay following the discovery of a breach. Data breaches are logged, tracked, and resolved in a timely manner in accordance with organizational policies and procedures.	Breach Notification	Compliant	
CTL12282	The organization identifies and documents the relevant basis for the international transfer of personal data. In addition, on an ongoing basis, the organization monitors and acts on any changes that affect the legality or performance of international transfers.	Data Privacy Policy Employee Training Status Report Policy Review Note	Compliant	