



APPTROVE

12 JULY 2024

A Self Attestation Report on
Controls Relevant to GDPR



Self-Attestation by



AKITRA

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):	GDPR
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://approve.com/terms-of-service/>

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

Our billing policy <https://approve.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	Datastore	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:

Approve has a staff of 35 employees and contractors.

3.4 Security Processes and Procedures:

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

3.5 Data:

- Customer's personal data - Approve 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 services, which is confidential and sensitive information, collected and retained within Approve database. But the said sensitive information is just used by you as a Approve user for gaining access to the services and is not used or accessed by Approve 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.

a) 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 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 GDPR. 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

Our self-attestation covers the following key areas:

1. **Data Protection Policies:** Detailed descriptions of the data protection policies and procedures adopted by our organization.
2. **Data Processing Activities:** An overview of how we collect, process, and manage personal data, including the legal basis for processing and data retention practices.
3. **Data Subject Rights:** Procedures established to ensure that individuals can exercise their rights under the GDPR, including access, rectification, and erasure of personal data.
4. **Data Security Measures:** Description of the technical and organizational measures implemented to protect personal data against unauthorized access, alteration, or destruction.
5. **Training and Awareness:** Information on the training provided to staff to ensure awareness and understanding of GDPR requirements and data protection responsibilities.

➤ 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 GDPR 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:

1. Obtaining an understanding of the service organization's service commitments and system requirements.
2. Assessing the risks that the controls were not suitably designed or did not operate effectively.
3. Performing procedures to obtain evidence about whether the controls are implanted as per standard criteria.
4. 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.

- Akitra Team

➤ Section 7: Audit Details

Control ID.	Control Description	Findings	Compliance Status	Remark
CTL121	The entity has obtained Implicit or explicit consent from data subjects at or before the time personal information is collected or soon thereafter	<ol style="list-style-type: none"> 1. Data Privacy Policy 2. Data Retention Policy 	Compliant	No Exception
CTL122	The entity has obtained implicit or explicit consent prior to a new use or purpose, If personal information that was previously collected is to be used for purposes not previously mentioned in the privacy notice	<ol style="list-style-type: none"> 1. Data Privacy Policy 2. Data Retention Policy 	Compliant	No Exception
CTL123	The entity obtains explicit consent directly from the data subject when sensitive personal information is collected, used, or disclosed	<ol style="list-style-type: none"> 1. Data Privacy Policy 2. Data Retention Policy 	Compliant	No Exception
CTL124	The organization has the procedure to obtain consent before personal information is transferred to or from an individual's computer or similar device	<ol style="list-style-type: none"> 1. Data Privacy Policy 2. Data Retention Policy 3. Cookies Accept 	Compliant	No Exception
CTL125	The organization collects personal information that is limited and is consistent with its objectives	Data Privacy Policy	Compliant	No Exception

CTL126	The organization has reviewed the personal information collected by different methods before they are implemented in order to confirm that personal information is obtained fairly	Data Privacy Policy	Compliant	No Exception
CTL127	The organization has defined policies and procedures to confirm that third parties from whom personal information is collected are reliable sources that collect information fairly and lawfully	Data Privacy Policy	Compliant	No Exception
CTL128	The organization informs data subjects when additional information is acquired about them for its use	Data Privacy Policy	Compliant	No Exception
CTL129	The organization obtains explicit consent directly from the data subject when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise	Data Privacy Policy	Compliant	No Exception
CTL130	The organization has defined objectives related to privacy for retaining documentation of explicit consent for the collection, use, or disclosure of sensitive personal information.	Data Privacy Policy	Compliant	No Exception

CTL131	The organization uses the personal information only for the intended purposes for which it was collected and only after implicit or explicit consent has been obtained	Data Privacy Policy	Compliant	No Exception
CTL132	The organization retains personal information no longer than necessary to fulfill the stated purposes	Data Privacy Policy Data Retention Policy	Compliant	No Exception
CTL148	The organization creates and maintains a record of authorized disclosures of personal information that is complete, accurate, and timely	Data Privacy Policy Data Retention Policy	Compliant	No Exception
CTL149	The organization creates and maintains a record of detected or reported unauthorized disclosures of personal information	Data Privacy Policy Data Retention Policy	Compliant	No Exception
CTL150	The organization has an agreements in place with third parties for disclosure of personal information to those parties	Data Privacy Policy Data Retention Policy Vendor Agreement Template	Compliant	No Exception
CTL151	The organization has defined a process for assessment of vendors' and other third parties' compliance with personal information disclosure terms, and has defined remedial action in response to	Data Privacy Policy Data Retention Policy Vendor Agreement Template	Compliant	No Exception

	the misuse of that personal information			
CTL152	Organization takes remedial action in response to unauthorized disclosure of personal information by vendors and other third parties	Data Privacy Policy Data Retention Policy	Compliant	No Exception
CTL153	Organization maintains agreements with its vendors and other third parties, which require notifying the organization in the event of any actual or suspected misuse of personal information	Data Privacy Policy Data Retention Policy Vendor Agreement Template	Compliant	No Exception
CTL154	Remedial action is taken in response to the misuse of personal information	Breach Notification Breach Policy Security Incident Response Policy	Compliant	No Exception
CTL155	The organization has defined a process for providing notice of breaches and incidents to the affected data subjects and, where appropriate or required, to regulators, to meet the objectives related to privacy.	Data Privacy Policy Security Incident Response Policy	Compliant	No Exception
CTL156	For each data subject, the organization tracks the personal information that it holds or that it has disclosed to a third party	Data Privacy Policy Data Retention Policy	Compliant	No Exception

CTL157	The organization has a defined procedure for responding to data subjects' requests for an accounting of personal information held and of disclosures of that information. Information related to the requests is identified and communicated to data subjects.	Data Privacy Policy Data Retention Policy	Compliant	No Exception
CTL158	The organization collects complete, current and accurate personal information for the relevant purposes for which it is to be used, as defined in the agreements with data subjects	Data Privacy Policy Data Retention Policy	Compliant	No Exception
CTL160	The organization has a process in place to address privacy inquiries, complaints and disputes.	Data Privacy Policy Data Retention Policy	Compliant	No Exception
CTL25	Change scope, change type, and roles and responsibilities are pre-established and control workflow, notification and approval requirements are also pre-established based on risk associated with change scope and type.	Change statement System Change Policy	Compliant	No Exception
CTL27	The organization defines external communication requirements for incidents, including: - information about	Breach Notification Security Incident Response Policy	Compliant	No Exception

	<p>external party dependencies - criteria for notification to external parties as required by the organization policy in the event of a security breach - contact information for authorities (e.g., law enforcement, regulatory bodies, etc.) - provisions for updating and communicating external communication requirement changes</p>			
<p>CTL28</p>	<p>The organization defines the types of incidents that need to be managed, tracked and reported, including: - procedures for the identification and management of incidents - procedures for the resolution of confirmed incidents - key incident response systems - incident coordination and communication strategy - contact method for internal parties to report incidents - support team contact information - notification to relevant management in the event of a security breach - provisions for updating and communicating</p>	<p>Incident Tracker</p>	<p>Compliant</p>	<p>No Exception</p>

	the plan - provisions for training of support team - preservation of incident information - management review and approval, (in accordance with frequency), or when major changes to the organization occur			
CTL48	Changes to the production environment are implemented by authorized personnel.	Change statement Product Access List System Change Policy	Compliant	No Exception
CTL53	The organization changes shared data encryption keys - at the end of the (organization-defined lifecycle period) - when keys are compromised - upon termination/transfer of employees with access to the keys	Access proof Incident Tracker	Partially compliant	Old Evidence Attached
CTL62	The organization's data classification criteria are reviewed, approved by management, and communicated to authorized personnel (in accordance with the organization-defined frequency), the data security management determines the treatment of data according to its designated data classification level.	DATA CLASSIFICATION POLICY Employee Training Status Report Policy Review Note	Compliant	No Exception
CTL147	The organization has a procedure for disclosing personal	Data Privacy Policy Data Retention Policy	Complaint	No Exception

	information to third parties for new purposes or uses, but only with the prior explicit consent of data subjects			
CTL161	The organization has mechanisms to address each privacy complaint or dispute, and the resolution is documented and communicated to the individual who made the complaint	Data Privacy Policy, Data Retention Policy	Compliant	No Exception
CTL162	The organization periodically reviews documentation of and compliance with objectives related to privacy. The organization has defined ongoing procedures for monitoring the effectiveness of controls over personal information	Data Privacy Policy, Data Retention Policy	Compliant	No Exception
CTL214	The organization provides a privacy notice to data subjects, at or before the time personal information is collected	Cookies Accept, Data Privacy Policy, Privacy Acknowledgement	Compliant	No Exception
CTL215	The organization captures the request for deletion of personal information, and information related to the requests is identified and flagged for destruction to meet The organization's objectives related to	Data Privacy Policy, Data Retention Policy	Compliant	No Exception

	privacy.			
CTL216	When provided by data subjects, The organization updates or corrects personal information that it holds or has provided to third parties	Data Privacy Policy, Data Retention Policy	Compliant	No Exception
CTL217	Personal information is disclosed only to third parties who have agreements with The organization to protect personal information in a manner consistent with the relevant aspects of The organization's privacy notice	Data Privacy Policy, Data Retention Policy	Compliant	No Exception
CTL140	The organization informs data subjects in a timely manner if they are denied access to their personal information when they request it, along with the reason for the denial, unless prohibited by law or regulation	Data Privacy Policy Data Retention Policy	Complaint	No Exception
CTL141	The organization has a legal, contractual right to deny data subjects' requests to access their personal information	Data Privacy Policy Data Retention Policy	Complaint	No Exception

CTL145	The organization has a procedure for providing personal information to third parties only for the purposes for which it was collected or created and only when implicit or explicit	Data Privacy Policy Data Retention Policy	Complaint	No Exception
--------	---	--	-----------	--------------

	consent has been obtained from the data subject			
CTL143	Data subjects are informed, in writing, about the reason a request for correction of personal information was denied and how they may appeal	Data Privacy Policy Data Retention Policy	Complaint	No Exception
CTL144	The organization has a procedure for communicating privacy policies or other specific instructions or requirements for handling personal information to third parties	Data Privacy Policy Data Retention Policy	Complaint	No Exception
CTL133	The organization has defined policies and procedure to protect personal information from erasure or destruction during the specified retention period of the information.	Data Privacy Policy Data Retention Policy	Compliant	No Exception

CTL135	The organization ensures that personal information which is longer retained by the organization is anonymized or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.	Data Privacy Policy Data Retention Policy	Compliant	No Exception
CTL136	The organization has defined policies and procedures to erase or otherwise destroy personal information that has been	Data Retention Policy	Compliant	No Exception

	identified for destruction.			
CTL137	The organization maintains an authentication procedure to authenticate the identity of data subjects who request access to their personal information, prior to giving them access to that information	Data Privacy Policy Data Retention Policy	Compliant	No Exception
CTL138	The organization allows data subjects to determine whether it maintains personal information about them and, upon request, provides access to the information.	Data Privacy Policy Data Retention Policy	Compliant	No Exception

CTL139	The organization provides personal information to data subjects in an understandable form, in a reasonable time frame, and at a reasonable cost, if any	Data Privacy Policy Data Retention Policy	Compliant	No Exception
CTL63	Logical access provisioning to information systems requires approval from appropriate personnel.	Access proof Access Control Policy	Partially compliant	Old Evidence Attached
CTL64	Logical access that is no longer required in the event of a termination is documented, communicated to management, and revoked.	Access revoke Asset Return proof	compliant	No Exception

CTL117	The organization has a well-defined privacy notice which is conspicuous and uses clear language	Data Privacy Policy Employee Privacy Policy and Notice (Latest)	Compliant	No Exception
CTL118	The organization's privacy notice describes the objectives of the entity and the activities covered by the notice	Data Privacy Policy Employee Privacy Policy and Notice (Latest)	Compliant	No Exception
CTL119	The entity has a defined procedure to inform the data subjects about their available choices with respect to the collection, use and disclosure of personal information	Cookies Accept Data Privacy Policy Privacy Acknowledgement Terms acknowledgement	Compliant	No Exception

CTL120	The entity has a procedure to inform the data subjects of the consequences of refusing to provide personal information for the purpose identified in the notice (this does not seem relevant to what the criterion requires -- it belongs with 3.2-1)	Privacy Acknowledgement Data Privacy Policy	Compliant	No Exception
CTL1	The organization Management ensures that its organization is aligned with the corporate strategy by assigning key managers with responsibilities to execute the corporate strategy.	Organization chart, Roles Policy	Compliant	No Exception

CTL5	The organization has established a check-in performance management process for on-going dialogue between managers and employees. (In accordance with the organization-defined frequency) reminders are sent to managers to perform their regular check-in conversation.	Performance review, MOM Proof of 1 on 1 calendar invite	Compliant	No Exception
CTL11	(The organization-defined security leader) conducts a periodic staff meeting to communicate and align on relevant security threats, program performance, and resource prioritization.	Security Review Meeting Minutes	Compliant	No Exception

CTL14	The organization performs a risk assessment to determine the data types that can be shared with a managed service provider.	Risk Assessment Policy, Vendor Management Policy, Vendor Risk Assessment Report	Compliant	No Exception
CTL15	(In accordance with the organization-defined frequency), management reviews controls within third party assurance reports to ensure that they meet organizational requirements, if control gaps are identified in the	Vendor Management Policy, Vendor Risk Assessment Report	Compliant	No Exception

	assurance reports, management takes action to address impact the disclosed gaps have on the organization.			
CTL20	The design and operating effectiveness of internal controls are continuously evaluated against the established (organization-defined controls framework) by the organization. Corrective actions related to identified deficiencies are tracked to resolution.	Risk Assessment Policy, Risk Assessment Report	Compliant	No Exception

CTL218	The organization has a procedure, disclosed to data subjects, about how to contact The organization with inquiries, complaints, and disputes related to privacy	Data Privacy Policy Data Retention Policy	Compliant	No Exception
--------	---	---	-----------	--------------