AKITRA

Fastest Path to Customer Trust with Security Compliance Automation

CONFIDENTIAL REPORT

CCPA READY

CCPA Self Attestation Audit Report

TRACKIER®

Trackier

July 12, 2025

Audit Date

July 12, 2024 to July 11, 2025
Next Audit Window: July 12,2025 to July 11,2026

Table of Contents

DISCLAIMER

Akitra, Inc.
830 Stewart Dr Ste 269, Sunnyvale, CA 94085

The purpose of the report is to verify the Trackier conformance with the implementation and effectiveness of security controls in accordance with CCPA. The content of this report applies only to matters, which were evident to Akitra auditor at the time of the audit within the audit scope. Akitra accepts no liability whatsoever for consequences to, or actions taken by, third parties as a result of or in reliance upon information contained in this report. This audit is based on a sampling process.

Self Attestation Audit Report

➢Section 1: Organization information

Company name:	**Trackier**
Contract Person:	Aman Khatri
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
Website:	https://trackier.com/
Total number of employees:	121
Total number of employees within the scope:	121

➢ Section 2: Audit information

Audit standard(s):	**CCPA**
Audit type:	**Self Attestation Audit**
Date(s) of audit(s):	July 12, 2025
Duration:	Point in time audit.
Site(s) audited:	None
Audit team:	Akitra Internal Audit Team

➢ Section 3: System Description

INSTRUCTIONS:

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

Trackier uses advanced technology and a customer-first approach to help marketers across the globe build great products, create exceptional experiences, and preserve customer privacy. We have 3 different SaaS products
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.
b) Affnook - One powerful iGaming affiliate marketing platform to improve affiliate engagement, automate workflows, track performance, and deter fraud. All at one place.
c) Performance Marketing Platform - Track campaign metrics and manage payouts of different affiliates along with monitoring their performance

DC 2: The principal service commitments and system requirements

Our terms of service - https://Trackier.com/terms-of-service/

Privacy policy - https://Trackier.com/privacy-policy/

Our billing policy - https://Trackier.com/billing-policy/

Our SLAs

Working hours

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

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	SaaS, Android 6 & IOS 12	Zoho People	Employee information

Finance System	Payroll data	Purchased	SaaS, Android 6 & IOS 12	Zoho Payroll	Employee's payroll
Tech Team	Version Controlling	Purchased	SaaS, Android 6 & IOS 12	Github	Code hosting and sharing
Tech team	Build, test, and deploy their software.	Purchased	SaaS, Android 6 & IOS 12	Jenkins	Code Build
Billing Software	Customer's billing	Developed	SaaS, IOS 12	CloudStuff Technology	To manage customer's billing and invoice

3.2 People:

Trackier has a staff of 121 employees and contractors.

3.3 Security Processes and Procedures:

Privacy policy - https://Trackier.com/privacy-policy/

3.4 Data:

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

3.5 Third Party Access:

Trackier ensures that any third-party access to consumer data complies with the California Consumer Privacy Act (CCPA). Only authorized personnel, such as the Head of Engineering and designated lead engineers, can access production systems — and only for specific operational needs like debugging. All third-party service providers (e.g., AWS, Segment, Intercom) are categorized as service providers under CCPA and operate under data processing agreements (DPAs) that restrict data use strictly to the scope defined by Trackier and its customers. No personal information is sold or shared without explicit consent. Additionally, Trackier provides mechanisms for data deletion and access requests, ensuring that third parties also support consumer rights as required under CCPA.

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

Product list -

Trackier uses advanced technology and a customer-first approach to help marketers across the globe build great products, create exceptional experiences, and preserve customer privacy. We have 3 different SaaS products

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.

b) **Affnook** - One powerful iGaming affiliate marketing platform to improve affiliate engagement, automate workflows, track performance, and deter fraud. All at one place.

c) **Performance Marketing Platform** - Track campaign metrics and manage payouts of different affiliates along with monitoring their performance

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)
Trackier conducts background verification for all internal employees as part of its hiring and onboarding process. These checks comply with relevant local and international laws and are tailored based on role criticality and information sensitivity. The process includes criminal history checks (where permitted), identity verification, and employment history validation using both automated tools and manual review.

Background Check Process (BC2)
For third-party vendors, consultants, or contractors with privileged or technical access to Trackier systems, background checks are a prerequisite. These parties must provide evidence of recent verification or undergo background checks facilitated by Trackier. The assessment is risk-based and focuses on verifying identity, criminal records, and past affiliations, ensuring all personnel accessing sensitive data meet Trackier's security standards.

DC 6: Complementary User Entity Controls (CUECs):

Trackier'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 Trackier's services to be solely achieved by Trackier's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Trackier.

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 IDs	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 Trackier receives and reviews the GCP SOC 2 report annually. In addition, through its operational activities, Trackier 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 Trackier. Therefore, each user entity's internal control must be evaluated in

conjunction with Trackier'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 Trackier 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: Trackier

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:

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

Article ID	Article	CTL ID	Control Description	Test Applied by the Service Auditor	Test Results
ART- 5	Principles Relating to Processing of Personal Data	CTL12267	Employees and contractors are required to complete an information security and privacy awareness training as part of the onboarding process and annually thereafter.	Reviewed the Employee Training Policy, HR Security Policy, and Training Status Report to verify onboarding and annual training requirements; confirmed that all required training has been completed by all employees. However, one employee has not completed the training due to being on an approved sabbatical. The training will be completed upon their return.	Noted Exception
		CTL12268	The organization retains personal information consistent with its privacy commitments and as long as it is required for its intended purpose.	Reviewed the Data Retention Policy and Privacy Policy to verify that personal information is retained in accordance with privacy commitments and only as long as needed for its intended purpose.	No Exception

ART- 7	Conditions for Consent	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.	Reviewed Cookies Accept, Data Privacy Policy, Privacy Acknowledgement, Website Privacy Policy, and Terms Acknowledgement to verify that explicit consent is obtained and maintained prior to collection or new use/disclosure of personal information, and that mechanisms exist for data subjects to modify or withdraw consent.	No Exception
		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.	Reviewed the Data Privacy and Retention Policies to verify procedures for handling consent withdrawal requests; confirmed that relevant employee training has been completed.	No Exception
ART-8	Conditions applicable to child's consent in relation to information society services	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.	Reviewed Cookies Accept, Data Privacy Policy, Privacy Acknowledgement, Website Privacy Policy, and Terms Acknowledgement to verify that explicit consent is obtained and maintained prior to collection or new use/disclosure of personal information, and that mechanisms exist for data subjects to modify or withdraw consent.	No Exception

		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.	Reviewed the Data Privacy and Retention Policies to verify procedures for handling consent withdrawal requests; confirmed that relevant employee training has been completed.	No Exception
ART- 12	Transparent Information, Communication and Modalities for the exercise of the rights of the Data Subject	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 acknowledged by the employees and contractors on at least an annual basis or during significant changes.	Reviewed the Data Privacy Policy, Employee Privacy Notice, and related HR and training documents to confirm communication of privacy obligations; confirmed that employee acknowledgment and training have been completed as required. However, one employee has not completed the training due to being on an approved sabbatical. The training will be completed upon their return.	Noted Exception
		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.	Reviewed the published website privacy policy, Policy Review Notes, and employee privacy notice to confirm alignment with legal requirements and annual review; confirmed that employee training and awareness activities have been completed in accordance with policy requirements.	No Exception

		CTL12273	Requests received from controllers regarding exercising rights of data subjects are documented, retained, and acted upon without undue days.	Reviewed the Data Privacy Policy to verify that requests from controllers to exercise data subject rights are documented, retained, and acted upon without undue delay.	No Exception
ART-13	Information to be provided where Personal Data are collected from the Data Subject	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 acknowledged by the employees and contractors on at least an annual basis or during significant changes.	Reviewed the Data Privacy Policy, Employee Privacy Notice, and related HR and training documents to confirm communication of privacy obligations; confirmed that employee acknowledgment and training have been completed as required. However, one employee has not completed the training due to being on an approved sabbatical. The training will be completed upon their return.	Noted Exception
		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.	Reviewed the published website privacy policy, Policy Review Notes, and employee privacy notice to confirm alignment with legal requirements and annual review; confirmed that employee training and awareness activities have been completed in accordance with policy requirements.	No Exception
		CTL12273	Requests received from controllers regarding exercising rights of data subjects are documented, retained, and acted upon without undue days.	Reviewed the Data Privacy Policy to verify that requests from controllers to exercise data subject rights are documented, retained, and acted upon without undue delay.	No Exception

ART-14	Information to be provided where Personal Data have not been obtained from the Data Subject	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 acknowledged by the employees and contractors on at least an annual basis or during significant changes.	Reviewed the Data Privacy Policy, Employee Privacy Notice, and related HR and training documents to confirm communication of privacy obligations; confirmed that employee acknowledgment and training have been completed as required. However, one employee has not completed the training due to being on an approved sabbatical. The training will be completed upon their return.	Noted Exception
		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.	Reviewed the published website privacy policy, Policy Review Notes, and employee privacy notice to confirm alignment with legal requirements and annual review; confirmed that employee training and awareness activities have been completed in accordance with policy requirements.	No Exception
		CTL12273	Requests received from controllers regarding exercising rights of data subjects are documented, retained, and acted upon without undue days.	Reviewed the Data Privacy Policy to verify that requests from controllers to exercise data subject rights are documented, retained, and acted upon without undue delay.	No Exception

ART-15	Right of Access by the Data Subject	CTL12273	Requests received from controllers regarding exercising rights of data subjects are documented, retained, and acted upon without undue days.	Reviewed the Data Privacy Policy to verify that requests from controllers to exercise data subject rights are documented, retained, and acted upon without undue delay.	No Exception
ART-16	Right to Rectification	CTL12273	Requests received from controllers regarding exercising rights of data subjects are documented, retained, and acted upon without undue days.	Reviewed the Data Privacy Policy to verify that requests from controllers to exercise data subject rights are documented, retained, and acted upon without undue delay.	No Exception
ART-17	Right to Erasure ("Right to be forgotten")	CTL12273	Requests received from controllers regarding exercising rights of data subjects are documented, retained, and acted upon without undue days.	Reviewed the Data Privacy Policy to verify that requests from controllers to exercise data subject rights are documented, retained, and acted upon without undue delay.	No Exception
ART-18	Right to Restriction of Processing	CTL12273	Requests received from controllers regarding exercising rights of data subjects are documented, retained, and acted upon without undue days.	Reviewed the Data Privacy Policy to verify that requests from controllers to exercise data subject rights are documented, retained, and acted upon without undue delay.	No Exception

ART-19	Notification Obligation regarding Rectification or Erasure of Personal Data or Restriction of processing	CTL12273	Requests received from controllers regarding exercising rights of data subjects are documented, retained, and acted upon without undue days.	Reviewed the Data Privacy Policy to verify that requests from controllers to exercise data subject rights are documented, retained, and acted upon without undue delay.	No Exception
ART-20	Right to Data Portability	CTL12273	Requests received from controllers regarding exercising rights of data subjects are documented, retained, and acted upon without undue days.	Reviewed the Data Privacy Policy to verify that requests from controllers to exercise data subject rights are documented, retained, and acted upon without undue delay.	No Exception
ART-21	Right to Object	CTL1 2273	Requests received from controllers regarding exercising rights of data subjects are documented, retained, and acted upon without undue days.	Reviewed the Data Privacy Policy to verify that requests from controllers to exercise data subject rights are documented, retained, and acted upon without undue delay.	No Exception
ART-22	Automated Individual Decision-Making, including Profiling	CTL12273	Requests received from controllers regarding exercising rights of data subjects are documented, retained, and acted upon without undue days.	Reviewed the Data Privacy Policy to verify that requests from controllers to exercise data subject rights are documented, retained, and acted upon without undue delay.	No Exception

ART-23	Restrictions	CTL12273	Requests received from controllers regarding exercising rights of data subjects are documented, retained, and acted upon without undue days.	Reviewed the Data Privacy Policy to verify that requests from controllers to exercise data subject rights are documented, retained, and acted upon without undue delay.	No Exception
ART-24	Responsibility of the Controller	CTL12267	Employees and contractors are required to complete an information security and privacy awareness training as part of the onboarding process and annually thereafter.	Reviewed the Employee Training Policy, HR Security Policy, and Training Status Report to verify onboarding and annual training requirements; confirmed that all required training has been completed by all employees. However, one employee has not completed the training due to being on an approved sabbatical. The training will be completed upon their return.	Noted Exception
		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.	Reviewed the Data Privacy Policy, HR Security Policy, and Policy Review Notes to verify policy establishment and annual review; confirmed that the policy has been communicated through training to all employees.	No Exception
		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.	Reviewed the Encryption Policy, evidence of encryption at rest and in transit, and Security Review Meeting Minutes to confirm implementation of security measures and periodic assessment with timely remediation of identified issues.	No Exception

ART-25	Data Protection by design and by default	CTL12267	Employees and contractors are required to complete an information security and privacy awareness training as part of the onboarding process and annually thereafter.	Reviewed the Employee Training Policy, HR Security Policy, and Training Status Report to verify onboarding and annual training requirements; confirmed that all required training has been completed by all employees. However, one employee has not completed the training due to being on an approved sabbatical. The training will be completed upon their return.	Noted Exception
		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.	Reviewed the Data Privacy Policy, HR Security Policy, and Policy Review Notes to verify policy establishment and annual review; confirmed that the policy has been communicated through training to all employees.	No Exception
		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.	Reviewed the Encryption Policy, evidence of encryption at rest and in transit, and Security Review Meeting Minutes to confirm implementation of security measures and periodic assessment with timely remediation of identified issues.	No Exception

ART-27	Representatives of Controllers or Processors not established in the Union	CTL12276	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.	Reviewed the Data Privacy Policy, DPO Job Description, and Roles Policy to verify that an EU representative is designated to fulfill GDPR obligations and interface with supervisory authorities and data subjects.	No Exception
ART-28	Processor	CTL12267	Employees and contractors are required to complete an information security and privacy awareness training as part of the onboarding process and annually thereafter.	Reviewed the Employee Training Policy, HR Security Policy, and Training Status Report to verify onboarding and annual training requirements; confirmed that all required training has been completed by all employees. However, one employee has not completed the training due to being on an approved sabbatical. The training will be completed upon their return.	Noted Exception
		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.	Reviewed the Encryption Policy, evidence of encryption at rest and in transit, and Security Review Meeting Minutes to confirm implementation of security measures and periodic assessment with timely remediation of identified issues.	No Exception

		CTL12277	Organization obtains formal authorization from the controller prior to engaging another processor (sub-processor) to support its processing activities. Arrangements between processor and sub-processors are supported by written contracts outlining the same data protection obligations as it has with the controller.	Reviewed the Vendor Management Policy to verify that formal authorization from the controller is required before engaging sub-processors, and that written contracts include equivalent data protection obligations.	No Exception
		CTL12278	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.	"Reviewed the Risk Assessment Report, Vendor Agreement Template, Vendor Management Policy, and Vendor Risk Assessment Report to verify that written contracts with controllers define required security and privacy measures for processing personal data.	No Exception
ART-30	Records of Processing Activities	CTL12279	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.	Reviewed Security Review Meeting Minutes and the Data Classification Policy to verify that a record of processing activities is maintained, reviewed annually by management, and available to legal authorities upon request.	No Exception

ART-32	Security of Processing	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.	Reviewed the Encryption Policy, evidence of encryption at rest and in transit, and Security Review Meeting Minutes to confirm implementation of security measures and periodic assessment with timely remediation of identified issues.	No Exception
ART-33	Notification of a Personal Data Breach to the Supervisory Authority	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.	Reviewed the Business Continuity and Disaster Recovery Policy, Policy Review Note, Risk Assessment Policy, Risk Assessment Report, and Tabletop Exercise to verify that data breach risk assessments are conducted post-incident to determine compromise likelihood and notification requirements.	No Exception
		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.	Reviewed the Breach Notification policy to verify that personal data breaches are logged, tracked, resolved, and notified to controllers without unreasonable delay, in accordance with organizational procedures.	No Exception

ART-34	Communication of a Personal Data Breach to the Data Subject	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.	Reviewed the Business Continuity and Disaster Recovery Policy, Policy Review Note, Risk Assessment Policy, Risk Assessment Report, and Tabletop Exercise to verify that data breach risk assessments are conducted post-incident to determine compromise likelihood and notification requirements.	No Exception
ART-44	General Principle for Transfers	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.	Reviewed the Data Privacy Policy and Policy Review Notes to verify documentation of the legal basis for international data transfers and monitoring of related regulatory changes; confirmed that relevant employee training has been completed.	No Exception
ART-45	Transfers on the basis of an Adequacy Decision	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.	Reviewed the Data Privacy Policy and Policy Review Notes to verify documentation of the legal basis for international data transfers and monitoring of related regulatory changes; confirmed that relevant employee training has been completed.	No Exception
ART-46	Transfers Subject to Appropriate Safeguards	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	Reviewed the Data Privacy Policy and Policy Review Notes to verify documentation of the legal basis for international data transfers and monitoring of related regulatory changes; confirmed that	No Exception

			transfers.	relevant employee training has been completed.	
		CTL12283	The organization has established and implemented a data transfer procedure that specifies processes and conditions on the transfer of personal data to third countries or international organizations. The procedure is approved by management and communicated to employees and contractors.	Reviewed the Data Transfer Procedure documentation to confirm management approval and defined processes for international data transfers; confirmed that the procedure has been communicated through training to all employees.	No Exception