People Data Labs

System and Organization Controls (SOC) 3

Report on Management's Assertion Related to its

PDL's Service System

Relevant to the Trust Services Criteria for Security Category

For the Period
October 01, 2021 to September 30, 2022

Together with
Independent Service Auditor's Report

Table of Contents

I. Independent Service Auditor's Report

Independent Service Auditor's Report

People Data Labs, Inc.

Scope

We have examined People Data Labs, Inc.'s accompanying assertion titled "Assertion of People Data Labs, Inc. Management" (assertion) that the controls within People Data Labs, Inc.'s PDL's Service System (system) were effective throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that People Data Labs, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*trust services criteria*).

Service Organization's Responsibilities

People Data Labs, Inc. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that People Data Labs, Inc.'s service commitments and system requirements were achieved. People Data Labs, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, People Data Labs, Inc. is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve People Data Labs, Inc.'s service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve People Data Labs, Inc.'s service commitments and system requirements based on the applicable trust services criteria.

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 engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management’s assertion that the controls within People Data Labs, Inc.’s PDL’s Service System were effective throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that People Data Labs, Inc.’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

JohansonGroup LLP

Colorado Springs, Colorado
November 01, 2022

II. Assertion of People Data Labs, Inc. Management

People Data Labs

Assertion of People Data Labs, Inc. Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the People Data Labs, Inc.'s PDL's Service System (system) throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that People Data Labs, Inc.'s service commitments and system requirements relevant to security, availability, confidentiality, and privacy were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of People Data Labs, Inc.'s PDL's Service System," (description) and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that People Data Labs, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

People Data Labs, Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the accompanying system description.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that People Data Labs, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

People Data Labs, Inc. Management
November 01, 2022

III. Description of PDL’s Service System

Description of PDL’s Service System

COMPANY BACKGROUND

Founded in 2015 by Henry Nevue and Sean Thorne, People Data Labs began as recruiting software, intended to help companies better understand and source candidates. People Data Labs builds B2B data for developers, engineers, and data scientists. People Data Labs empowers our clients to build and scale innovative data-driven products using 3 billion, highly-accurate B2B records. Every day, our clients use our data to build personal profiles, enrich person records, power predictive modeling, drive artificial intelligence, and build new tools to make their teams more efficient, productive, and successful We’re proud to be the preferred data partner to the data science and engineering teams building the next generation of data-driven products and services. People Data Labs is the single source of truth in B2B data serving enterprise and startup clients across a range of data-enabled businesses.

PDL was founded by a group of entrepreneurs from the SaaS space, with deep experience in data integration and simple, intuitive user experience, and is backed by Craft Ventures, Founders Fund, and Susa Ventures.

DESCRIPTION OF SERVICES OVERVIEW OR SERVICES PROVIDED

The People Data Labs API/Platform makes it incredibly easy for data teams and operators to enrich data from compliantly sourced datasets to augment their databases. PDL is delivered as a web API or licensed database. This allows engineering, data science, product, and other technical teams to build compliant, innovative, people-data-based software solutions.

PDL also provides tools for creating new data models via API queries, browsing existing data, and enriching data pipelines.

PDL is delivered as a web API or licensed database. This allows engineering, data science, product, and other technical teams to build compliant, innovative, people-data-based software solutions.

PDL also provides tools for creating new data models via API queries, browsing existing data, and enriching data pipelines.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

People Data Labs, Inc. designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that People Data Labs, Inc. makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that People Data Labs, Inc. has established for the services. The system services are subject to the Security, Confidentiality, Availability, Processing integrity, and Privacy commitments established internally for its services.

We communicate our system and service commitments via our website. We provide this information via our Terms of Service, Acceptable Use Policy, Privacy Policy, etc. Additionally, our certification programs (SOC2, type2, and ISO 27001) communicate our commitment to security. Upon request, we provide additional documentation via our Whistic implementation and trust catalog. Our SLA uptime is 99.95% and we have an RTO and RPO of 24 hours. We comply with CCPA, GPDR, and other legal requirements in our industry.

Security commitments

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Uptime availability of production systems

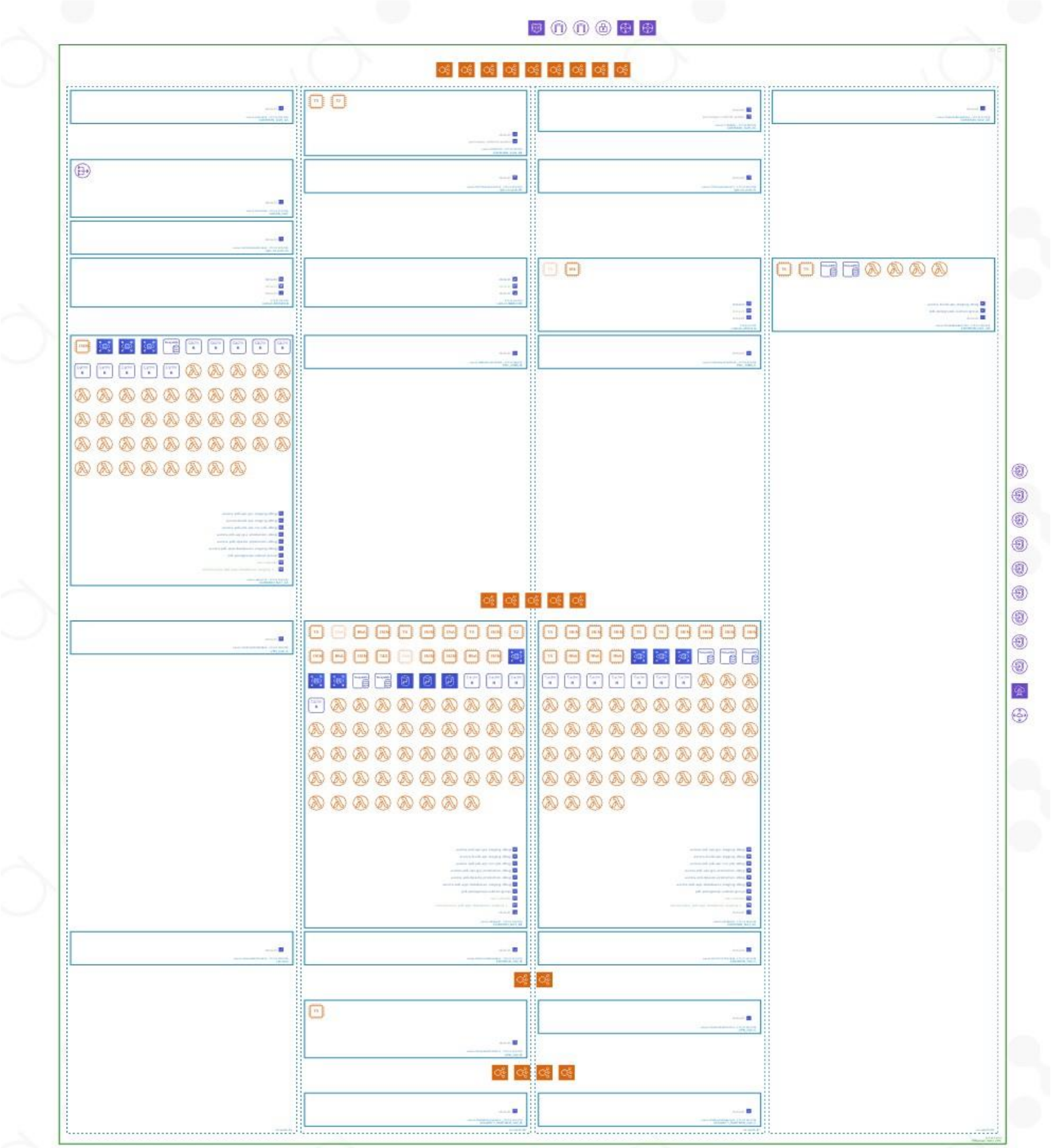
COMPONENTS OF THE SYSTEM

The System description is comprised of the following components:

- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Infrastructure

People Data Labs, Inc. maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents the device name, inventory type, description, and owner. To outline the topology of its network, the organization maintains the following network diagram(s).



Hardware	Type	Purpose
AWS Elastic Compute Cloud (EC2)	AWS	Scalable Computing Capacity
AWS Elastic Load Balancers	AWS	Load balance internal and external traffic
Virtual Private Cloud	AWS	Protects the network perimeter and restricts inbound and outbound access
S3 Buckets	AWS	Storage, upload and download

Software

People Data Labs, Inc. is responsible for managing the development and operation of the People Data Labs API system including infrastructure components such as servers, databases, and storage systems. The in-scope People Data Labs, Inc. infrastructure and software components are shown in the table provided below:

System/Application	Operating System	Purpose
GuardDuty	AWS	Security application used for automated intrusion detection (IDS)
Datadog	Datadog	Monitoring application used to provide monitoring, alter, and notification services for People Data Labs, Inc. platform
PostgreSQL	Linux	Transactional database
Redis	Linux	Used to maintain cached data

People

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

People Data Labs, Inc. has a staff of approximately 133 organized in the following functional areas:

Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.

This includes:

- CEO - Sean Thorne
- COO - Henry Nevue
- CTO - Alex Bahouth
- CPO - Varun Villait
- VP of Finance - Madeleine Stanley
- VP of People Enablement - Shane Price

Operations: Responsible for maintaining the availability of production infrastructure, and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.

Information Systems and Security: Responsible for managing laptops, software, and other technology involved in employee productivity and business operations. Responsible for all security configurations, audits, and documentation

Product Tech Team: Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

Sales and Customer Service: Responsible for Sales, Revenue, and customer support. The Customer Success Team is the first point of contact for communicating with the customers.

Data

Data as defined by People Data Labs, Inc., constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Company Proprietary Data (Internal) - This includes configuration data, logs, source code, and other information specific to People Data Labs operations. It also includes all information that is protected by NDA requirements.

Public Data - This includes websites, OpenSource SDKs, API documentation, and all documents that are publicly releasable.

Data is categorized into the following major types of data used by People Data Labs, Inc.

Category	**Description**	**Examples**
Public	Public information is not confidential and can be made public without any implications for People Data Labs, Inc..	• Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences
Customer data	Information received from customers for processing or storage by People Data Labs, Inc. People Data Labs, Inc. must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Customers' customers' PII

		• Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by People Data Labs, Inc. to operate the business. People Data Labs, Inc. must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All employees and contractors of the company are obligated to respect and, in all cases, protect customer data.

Additionally, People Data Labs, Inc. has policies and procedures in place for the proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

PROCESSES AND PROCEDURES

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Physical security

People Data Labs, Inc.'s production servers are maintained by AWS. The physical and environmental security protections are the responsibility of AWS. People Data Labs, Inc. reviews the attestation reports and performs a risk analysis of AWS on at least an annual basis.

Logical access

People Data Labs, Inc. provides employees and contracts access to infrastructure via a role-based access control system, to ensure uniform, least privileged access to identified users and to maintain simple and reportable user provisioning and de-provisioning processes.

Access to these systems is split into admin roles and user roles. User access and roles are reviewed on a quarterly basis to ensure the least privileged access.

Information Systems and Security is responsible for providing access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing People Data Labs, Inc.'s policies, and completing security training. These steps must be completed within 14 days of hire.

When an employee is terminated, Information Systems and Security are responsible for deprovisioning access to all in-scope systems within 3 days of that employee's termination.

Computer Operations - Backups

Customer data is backed up and monitored by the Platform for completion and exceptions. If there is an exception, Platform will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer Operations - Availability

People Data Labs, Inc. maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting, and acting upon breaches or other incidents.

People Data Labs, Inc. internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

People Data Labs, Inc. utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

Change Management

People Data Labs, Inc. maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

People Data Labs, Inc. has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the People Data Labs, Inc. application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The PaaS provider also automates the provisioning and de-provisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on the underlying hardware.

PDL employs AWS Inspector for vulnerability scanning software it checks containers and VM images, for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues. We utilize Snyk, Bandit, and other open-source tools for source code vulnerability and security scanning.

BOUNDARIES OF THE SYSTEM

The boundaries of the People Data Labs API are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the People Data Labs API.

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

THE APPLICABLE TRUST SERVICES CRITERIA AND THE RELATED CONTROLS

Common Criteria (to the Security Categories)
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

CONTROL ENVIRONMENT

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of People Data Labs, Inc.'s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of People Data Labs, Inc.'s ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

People Data Labs, Inc.'s management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

The People Data Labs, Inc. management team must balance two competing interests: continuing to grow and develop in a cutting-edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly-sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way People Data Labs, Inc. can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require People Data Labs, Inc. to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

Organizational Structure and Assignment Of Authority and Responsibility

People Data Labs, Inc.'s organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

People Data Labs, Inc.'s assignment of authority and responsibility activities includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity’s objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

HR policies and practices

People Data Labs, Inc.'s success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top-quality personnel who ensures the service organization is operating at maximum efficiency. People Data Labs, Inc.'s human resources policies and practices relating to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

RISK ASSESSMENT PROCESS

People Data Labs, Inc.'s risk assessment process identifies and manages risks that could potentially affect People Data Labs, Inc.'s ability to provide reliable and secure services to our customers. As part of this process, People Data Labs, Inc. maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular People Data Labs, Inc. product development process so they can be dealt with predictably and iteratively.

Integration with risk assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of People Data Labs, Inc.'s system; as well as the nature of the components of the system result in risks that the criteria will not be met. People Data Labs, Inc. addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meet the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, People Data Labs, Inc.'s management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

INFORMATION AND COMMUNICATION SYSTEMS

Information and communication are an integral component of People Data Labs, Inc.'s internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

People Data Labs, Inc. uses several information and communication channels internally to share information with management, employees, contractors, and customers. People Data Labs, Inc. uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, People Data Labs, Inc. uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

MONITORING CONTROLS

Management monitors control to ensure that they are operating as intended and that controls are modified as conditions change. People Data Labs, Inc.'s management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-going monitoring

People Data Labs, Inc.’s management conducts quality assurance monitoring on a regular basis and additional training is provided based on the results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management’s close involvement in People Data Labs, Inc.’s operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control’s weakness is made based on whether the incident was isolated or requires a change in the company’s procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of People Data Labs, Inc.’s personnel.

Reporting deficiencies

Our internal risk management tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

CHANGES TO THE SYSTEM

Implemented GitHub Enterprise
Implemented JIRA and Replace Notion with Confluence.
Major upgrade of services with Zoom
Added a Chief Technology Officer

INCIDENTS

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

CRITERIA NOT APPLICABLE TO THE SYSTEM

All Common Criteria/Security, Security, Confidentiality, Availability, Processing integrity, and Privacy criteria were applicable to the People Data Labs, Inc.'s People Data Labs API system.

SUBSERVICE ORGANIZATIONS

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

SUBSERVICE DESCRIPTION OF SERVICES

The Cloud Hosting Services provided by AWS support the physical infrastructure of the entity's services.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

Subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to People Data Labs, Inc.'s services to be solely achieved by People Data Labs, Inc. control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their internal controls or procedures to complement those of People Data Labs, Inc.

The following subservice organization controls have been implemented by AWS and included in this report to provide additional assurance that the trust services criteria are met.

AWS

Category	Criteria	Control
Security	CC 6.4	Physical access to data centers is approved by an authorized individual.
Security	CC 6.4	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
Security	CC 6.4	Physical access to data centers is reviewed on a quarterly basis by the appropriate personnel.
Security	CC 6.4	Closed-circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days unless limited by legal or contractual obligations.
Security	CC 6.4	Access to server locations is managed by electronic access control devices.

People Data Labs, Inc. management, along with the subservice provider, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, People Data Labs, Inc. performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization(s)
- Making regular site visits to vendor and subservice organization(s') facilities
- Testing controls performed by vendors and subservice organization(s)
- Reviewing attestation reports over services provided by vendors and subservice organization(s)
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

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

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.

1. User entities are responsible for understanding and complying with their contractual obligations to People Data Labs, Inc.
2. User entities are responsible for notifying People Data Labs, Inc. of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of People Data Labs, Inc. services by their personnel.
5. User entities are responsible for developing disaster recovery and business continuity plans that address the inability to access or utilize People Data Labs, Inc. services.
6. User entities are responsible for providing People Data Labs, Inc. with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying People Data Labs, Inc. of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfer