Report on Algolia, Inc.'s Search Solution System Relevant to Security, Availability, and Confidentiality Throughout the Period January 1, 2021 to December 31, 2021

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

Table of Contents

Section 1

Section 2

Attachment A

Attachment B

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Algolia, Inc. ("Algolia")

Scope

We have examined Algolia's accompanying assertion titled "Assertion of Algolia, Inc. Management" (assertion) that the controls within Algolia's Search Solution System (system) were effective throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that Algolia's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (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*).

The description of the boundaries of the system indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Algolia, to achieve Algolia's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of Algolia's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Algolia uses subservice organizations to provide data center colocation services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Algolia, to achieve Algolia's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Algolia's controls. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Algolia 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 Algolia's service commitments and system requirements were achieved. Algolia has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Algolia 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 Auditor's 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 Algolia'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 Algolia'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 examination 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 Algolia's Search Solution System were effective throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that Algolia's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Algolia's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Westminster, Colorado
April 6, 2022

Section 2

Assertion of Algolia, Inc. Management

Assertion of Algolia, Inc. (“Algolia”) Management

We are responsible for designing, implementing, operating and maintaining effective controls within Algolia’s Search Solution System (system) throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that Algolia’s service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Algolia, to achieve Algolia’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of Algolia’s controls.

Algolia uses subservice organizations for data center colocation services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Algolia, to achieve Algolia’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Algolia’s controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that Algolia’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (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) if complementary subservice organization controls and complementary user entity controls assumed in the design of Algolia’s controls operated effectively throughout that period. Algolia’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 attachment B.

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 January 1, 2021 to December 31, 2021, to provide reasonable assurance that Algolia's service commitments and system requirements were achieved based on the applicable trust services criteria.

Algolia, Inc.

Attachment A

Algolia, Inc.’s Description of the Boundaries of Its Search Solution System

Type of Services Provided

Since 2014, Algolia, Inc. (“Algolia” or “the Company”) has provided its Search Solution System to businesses of all sizes around the world. Algolia provides user entities (customers) a hosted and internally developed search solution to provide an end-to-end search experience for their applications and services.

The scope of Algolia’s Search Solution System includes all the products as listed below, the teams supporting the development and maintenance of these products, and the physical locations of Paris, France and San Francisco, CA.

The scope of services includes the following components of the Algolia Search Solution System:

Algolia Search

Algolia Search Application Programming Interface (API) is the internally-developed proprietary core of Algolia’s services. Algolia Search API is a schema-less JavaScript Object Notation (JSON) based search engine optimized for user-facing searches. Algolia Search API is operated in clusters, where servers cooperate using a distributed consensus protocol to ensure the consistency of the data and the availability of the service. Algolia Search API provides up to 99.99% availability through its distributed configuration.

To mitigate the impact of network latency, Algolia Search API provides the option to enrich the primary cluster by an arbitrary number of Distributed Search Network (DSN) servers that serve as read replicas. The users are then geo-routed to the closest server with the customer data. In addition to lowering network latency, this solution also improves the availability of the entire system by making it more resilient to region scale outages.

Internally, Algolia Search API uses an encrypted binary communication protocol between servers. Externally, Algolia exposes public Hypertext Transfer Protocol (HTTP) and HTTP Secure (HTTPS) interfaces for the Algolia Search API.

Algolia Dashboard

Algolia Dashboard is a web management interface that uses the Algolia Search API and provides a user-friendly interface for using and configuring the Algolia Search API. The dashboard also provides user management functionality.

The Algolia Dashboard is available using HTTPS with the HTTP Strict Transport Security preloaded in most modern browsers to eliminate the possibility of downgrade attacks that strip away the Transport Layer Security (TLS) of HTTPS connections.

Algolia Analytics & Insight

Algolia Analytics API is a JSON-based API that provides access to analytics data generated from queries. The queries performed through the Algolia Search API are collected, analyzed, and made available through this API, allowing the customer to analyze the user experience, trends, and impacts of changes.

Algolia Monitoring API

Algolia Monitoring API is an abstraction API for Algolia’s multiple monitoring systems that collects data about the usage and operations of the Algolia Search API. This API allows customers to get the data that is available in the Algolia Dashboard and is used for the Algolia status page.

Algolia Shopify

Algolia Shopify creates a personalized e-commerce site search and discovery experiences for shoppers.

Algolia Crawler (Algolia Site Search)

Algolia Crawler is a customized site search and discovery tool that automatically extracts and enhances website's content. It is a content discovery platform that enables businesses to build, manage and deliver customer centric, content-based experiences on every channel.

Algolia Personalization

Algolia Personalization help make users a personalized experience more compelling and relevant with Algolia.

Algolia Recommend

Algolia Recommend help to compose the recommendations experiences in the context of companies' applications. It builds applications quickly that automatically show products or digital content to its users, subscribers, and shoppers that complement and refine their current selection. This solution maximizes conversions and catalog exposure for online vendors.

The boundaries of the system in this section of the report details the Algolia Search Solution System. Any other Company services are not within the scope of this report.

The Boundaries of the System Used to Provide the Services

The boundaries of the Algolia Search Solution System 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 Algolia Search Solution System.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

Algolia operates its services on a physical and virtual infrastructure placed in third-party datacenters and colocation services of third-party server providers. The data centers hosting the services are located in US West (California), US Central (Texas), US East (Virginia), Canada (Montreal), South America (São Paulo), Europe (France, Netherlands and Germany), Russia (Moscow), South Africa, India, Singapore, Hong Kong, Japan (Tokyo and Osaka), Australia (Sydney), and the United Arab Emirates (Dubai). Portions of the provided services are hosted by various cloud providers, including OVH, Amazon Web Services (AWS), and Google Cloud Platform (GCP).

In order to increase the overall security of the system, Algolia has designed its network environment as a zero-trust network with traditional network concepts of external untrusted and internal trusted networks without a demilitarized zone (DMZ) network. In Algolia's environment, all networks are external and untrusted, and each server needs to be authorized to communicate together internally. Algolia's environment spans multiple data centers, multiple service providers, and multiple network autonomous systems while maintaining the security, resiliency, and availability of the service.

Algolia also operates the related network equipment supporting the infrastructure in locations where Algolia uses colocation services to place servers.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

Infrastructure		
Production Tool	**Business Function**	**Hosted Location**
Databases	Customer data storage	AWS and GCP
Kubernetes	Cluster Management	AWS
Virtual Private Cloud and Security Groups (Firewalls)	Protects the network perimeter and restricts inbound and outbound access.	AWS and GCP

Software

The environment of Algolia is based on Linux operating systems (OSs) and heavily utilizes open-source software. Algolia's environment is composed of multiple systems that offer the services to its customers and work in tandem with internal systems supporting the operations of the infrastructure.

Application Monitoring

Algolia uses multiple monitoring systems with redundant architectures including Pingdom, host-based monitoring, and its own purpose-built monitoring network. While Pingdom provides a high-level overview of system availability, Algolia's purpose-built monitoring network provides telemetry data about the availability of its services. This network is composed of multiple monitoring probes running around the world and constantly monitoring the Algolia infrastructure and its services. This data is then displayed live on Algolia's public automatic status page. No human intervention is necessary for the status page to display that the service is degraded or unavailable and all the data is also available in the monitoring API.

The application monitoring system also verifies the correctness of Algolia's services by performing end-to-end logic tests of the services. Algolia's monitoring network also monitors critical portions of the infrastructure, such as the Domain Name Server (DNS) service endpoints of Algolia's providers.

Infrastructure Monitoring

Every system in the Algolia environment is monitored, including infrastructure metrics such as central processing units (CPUs), memory, and network utilization. This data is then transparently collected and analyzed. Additional alerts are evaluated on top of this data to provide Algolia with proactive alerting that might impact the service before the actual degradation happens.

Backups and Disaster Recovery

Algolia has developed internal backup mechanisms that mirror the application data multiple times per day from the production servers to backup locations over an encrypted tunnel. Once the mirror is finished, local processing of the data is performed, and the consistency of the data is verified before further processing.

An encrypted backup is then generated and distributed to the recovery storage closest to the source cluster to provide the fastest possible recovery times.

All the databases are backed up daily using the appropriate database backup mechanisms to ensure the consistency of the backups.

Algolia also maintains a disaster recovery (DR) plan for its systems in case of a complete outage. The DR plan is tested at least annually. System failures that do not impact the availability of the Algolia service are continuously tested to ensure that all fallback and recovery mechanisms work as expected.

Logging

Algolia collects and maintains detailed logs from both the infrastructure and application level. These logs are centrally collected, analyzed, and respective alerts are evaluated. The collection of the logs is automatic. Additional application-specific collections are configured either by the configuration management tool or implicitly by producing the logs to Syslog.

Patch Management

All Algolia servers and running software are regularly patched. If the software allows it, automatic updates are enabled and security updates are installed automatically without intervention.

Integrity Monitoring

Algolia uses a host-based intrusion detection system (HIDS) to ensure the file integrity and protection of the systems from intrusion. The HIDS performs integrity tests of important files on the system and reports any changes. The HIDS uses its known signatures to regularly scan the systems for rootkits and other malware. HIDS alerts are centrally collected and analyzed.

The list of software and ancillary software used to build, support, secure, maintain, and monitor the Algolia Search Solution System include the following applications, as shown in the table below:

Software	
Production Application	**Business Function**
AWS and GCP	Backup and replication
Elastic Search and Kibana	Security information and event management (SIEM), logging system
Wavefront and Pingdom	Infrastructure monitoring
Chef	Patch management
Nessus	Vulnerability scanning
Google MDM, Mosyle, and Microsoft Intune	Mobile device management
Crowdstrike	Antivirus and intrusion detection
BambooHR	HRIS
Jira	Help desk and ticketing system
PagerDuty and Slack	Security event monitoring and infrastructure monitoring

Software	
Production Application	**Business Function**
Okta	Authentication
Duo	Authentication

People

The development and operations of the systems are the responsibility of the Research & Development organization unit of Algolia, which is led by the Chief Technology Officer (CTO) and Vice President (VP) of Engineering.

Engineering teams working on systems are given the necessary infrastructure and tools they need for system development, testing, and operations. These teams operate their systems on their own and are responsible for the availability and operations of the system.

The Engineering team, led by the Director of Infrastructure, works on the automation, maintenance, operations, and security of all systems in Algolia. This Engineering team also includes Algolia's Security team, which is responsible for developing and designing the secure practices of Algolia systems, performing internal training, and developing new systems to improve the overall security of Algolia.

The Product team leads the development of Algolia's services based on feedback from customers, market needs, and the future goals of Algolia.

The Director of Infrastructure, the CTO, the VP of Engineering, and the VP of Legal ensure Algolia's continuous compliance with all developed policies and legal requirements.

Human Resources (HR) contributes to the security of Algolia's systems by performing background checks on new employees, adding new employees to Active Directory, and revoking assigned rights during the termination process.

Procedures

Algolia utilizes automation for all its systems to help achieve security, recover from failures, administer, and provide an overview of its assets. In order to ease the adoption of internal policies and guide employees through the correct processes, Algolia includes as much as possible in internal applications, configuration management, and internal systems.

Algolia has developed policies that cover the needs of operations and nature of services provided. These policies are available to all employees of the Company, business partners, and customers. Each policy is versioned and changes are logged.

The default system and server security configurations of all Algolia systems are anchored in the configuration management system based on the Chef configuration management tool that reconfigures the system to a desired state using predefined and dynamic templates. The configuration management system also provides the functionality of service discovery, allowing Algolia to operate its systems in a zero-trust architecture.

The change management policy governs how changes are made to production. Most of the changes are performed by changing code or configurations in system-related Git code repositories. These changes are tested in testing environments, approved by an engineering peer, and then deployed to production. Algolia employs multiple methods of production software deployment depending on the criticality of the system, including cold restart, hot reload, blue-green deployment, canary deployment, gradual deployment based on service type, and regional deployment.

The automatic monitoring system can trigger critical alerts and notify the 24/7 on-call team to resolve immediate issues and restore service. The most critical applications, like Algolia Search API, can trigger alerts directly without the monitoring system if the monitoring system is unavailable.

Algolia has developed a policy specifying the requirements for its data centers. Verification of these requirements is performed through the monitoring of subservice organizations.

Algolia has developed a series of policies, procedures, and technical measures to deal with large-scale technical issues that could impact the availability of Algolia's services or a pandemic issue that could impact a significant portion of Algolia's employees operating the service.

The following table details the procedures as they relate to the operation of the Algolia Search Solution System:

Procedures	
Procedure	**Description**
Logical Access	How the Company restricts logical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical security deviations.
Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Mitigation	How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Data

Algolia's business does not rely on selling or reselling customer data. For this reason, Algolia has developed an environment that protects data and confidentiality of its customers.

Data Classification

Algolia has developed a data classification policy for both customers and its own data. Due to the implicit sensitivity of customer data, this data is classified as confidential and this classification carries with itself requirements for data protection and data handling.

Algolia Search

Algolia Search API works with semi-structured JSON-formatted objects received via Representational State Transfer (REST) API. This API is available via HTTP for legacy systems and HTTPS for modern systems, with TLS configuration and certificates from respected public certification authorities. This API follows HTTP standards and is usable as-is or through integration libraries that Algolia provides as open-source software.

The API features an authentication scheme that allows customers to generate and manage access keys with different levels of permissions. This authentication scheme contains security parameters that allow customers to generate access keys using communication with the service as well as locally (offline) without any contact with the service.

Upon reception, the data is formatted into a proprietary file format, distributed, and stored on Algolia servers. All modifications of the data are performed via the API and every interaction with the data is audited. These audit logs are used for auditing and accounting purposes. Once generated, the audit logs are processed in Algolia's log processing system, where necessary information is extracted, and the logs are stored for further analysis, incident response, and modification or improvement of the service.

Algolia Dashboard

Algolia Dashboard is a web application primarily built on top of the Algolia Search API that provides additional user management and authentication for management. Algolia Dashboard stores information about authorized users that were added by the customer.

Algolia Analytics & Insight

Algolia Analytics and Insight does not handle customer data records. Analytics API produces data generated from the usage and audit logs of the Algolia Search API. This allows customers to get visibility into search requests being performed by their systems or their users

Algolia Monitoring API

The Algolia Monitoring API does not allow data to be stored. The Algolia Monitoring API produces data collected from Algolia about the state of the service and makes that information available to customers.

Logging

All systems produce application and operations logs that are collected, processed, and stored in Algolia's systems. These logs are purged from the system following retention requirements.

Data Retention

When data is being requested for deletion via the API, it is made unavailable as soon as the system converges and marks the data as ready for garbage collection (data purge). During the next garbage collection, the data is purged from the system by removing the data from its data storage, making it unavailable. At this point, the data is no longer accessible to the customer or Algolia, cannot be restored, and will not be listed by any of the tools or APIs.

After the backup retention period expires, the data is also purged from the backup systems. All Algolia systems are designed to automatically remove data marked for deletion in a timeframe specified by the internal data retention and disposal policy.

Algolia has established processes to allow customers to request data to be deleted from all systems.

The Company keeps track of user activity in relation to the types of services customers and their users use, the configuration of their computers, and performance metrics related to their use of the services.

The Company logs information about customers and their users, including Internet Protocol (IP) address. Log files are immutable records of computer events about an OS, application, or user activity, which form an audit trail. These records may be used to assist in detecting security violations, performance problems, and flaws in applications.

Complementary User Entity Controls (CUECs)

The Company's controls related to the Algolia Search Solution System cover only a portion of overall internal control for each user entity of the Algolia Search Solution System. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls taking into account the related CUECs identified for the specific criterion. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls
CC2.1	• User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified timeframes. • Controls to provide reasonable assurance that the Company is notified of changes in: – User entity vendor security requirements – The authorized users list
CC2.3	• It is the responsibility of the user entity to have policies and procedures to: – Inform their employees and users that their information or data is being used and stored by the Company. – Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
CC6.1	• User entities grant access to the Company's system to authorized and trained personnel. • Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by Algolia.
CC6.4 CC6.5 CC7.2 A1.2	• User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

Algolia uses multiple data center colocation providers as a subservice organization for data center colocation services. Algolia's controls related to the Algolia's Search Solution System cover only a portion of the overall internal control for each user entity of the Algolia's Search Solution System. The description does not extend to the services provided by the subservice organizations that provide colocation services for IT infrastructure.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. CSOCs are expected to be in place at all subservice organizations related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. Subservice organizations' physical security controls should mitigate the risk of unauthorized access to the colocation facilities. Subservice organizations' environmental security controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

Algolia monitors these controls by obtaining and reviewing subservice organization SOC 2 and/or SOC 1 reports annually as they are available. Due to the wide variety of subservice organizations that are used by Algolia, not all of the organizations used for data center and data center colocation services have a readily available SOC 2 or SOC 1 report to inspect. Algolia accepts valid ISO 27001 and PCI DSS reports to determine adequate physical security controls. If none of the accepted reports are available, Algolia performs its own evaluation of the subservice organizations using evaluation questionnaires and walk-throughs of these sites annually to ensure the controls are compliant with Algolia's requirements, are in place, and are operating effectively.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the Algolia Search Solution System to be achieved solely by Algolia. Therefore, each user entity's internal control must be evaluated in conjunction with Algolia's controls taking into account the related CSOCs expected to be implemented at the subservice organizations as described below.

Criteria	Complementary Subservice Organization Controls
CC6.4	• Colocation service providers are responsible for restricting data center access to authorized personnel. • Colocation service providers are responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.5 CC6.7	• Colocation service providers are responsible for securely decommissioning and physically destroying production assets in its control.
CC7.2 A1.2	• Colocation service providers are responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers. • Colocation service providers are responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • Colocation service providers are responsible for overseeing the regular maintenance of environmental protections at data centers.

Data Center Service Providers

The datacenters that are carved out for purposes of this report are listed in the table below.

Subservice Organization	Monitoring Control Performed
Leaseweb	Obtain and review a SOC 1 and an ISO27001
Amazon Web Services (AWS)	Obtain and review a SOC 2 and/or an ISO27001
Google Cloud Platform	Obtain and review a SOC 2 and/or an ISO27001
IPTP	Obtain and review a SOC 1, and/or a SOC 2, and/or an ISO27001
Equinix	Obtain and review a SOC 1, and/or a SOC 2, and/or an ISO27001
Packet	Obtain and review a SOC 1 and/or a SOC 2, and/or an ISO27001, and/or an Algolia Walk-through
Internap	Obtain and review a PCI DSS and/or a SOC 2

Subservice Organization	Monitoring Control Performed
MaxiHost	Obtain and review an ISO27001, and/or Algolia Walk-through
Anexia	Obtain and review an ISO27001 and ISO9001
OVH	Obtain and review an ISO27001, and/or Algolia Walkthrough
Hetzner	Obtain and review an ISO27001
Zone Networks	Obtain and review an ISO27001
WAN Security	Obtain and review an ISO27001
E2E Networks	Obtain and review an ISO27001
Web Werks	Obtain and review PCI-DSS, and/or Algolia Walk-through with Questionnaires
Microsoft Azure	Obtain and review a SOC 2

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the Algolia Search Solution System. Commitments are communicated in the master subscription agreement (MSA) and Service Level Agreement.

System requirements are specifications regarding how the Algolia Search Solution System should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the Algolia Search Solution System include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• Algolia will maintain administrative physical, and technical safeguards for the security and integrity of the Algolia Search Solution System consistent with industry standard practices.	• Logical access standards • Employee provisioning and deprovisioning standards • Access reviews • Intrusion detection standards • Risk and vulnerability management standards • Configuration management • Incident handling standards • Change management standards • Vendor management
Availability	• Algolia will maintain a production system uptime of 99.99%.	• System monitoring • Backup and recovery standards
Confidentiality	• Algolia will maintain all customer data as confidential and will not disclose information to any unauthorized parties without written consent. • Algolia will use at least the same degree of reasonable care as it uses to safeguard its own confidential information.	• Data classification • Retention and destruction standards • Internal confidentiality standards • Information sharing standards