REPORT ON ALGOLIA, INC.’S SEARCH SOLUTION SYSTEM RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY FOR THE PERIOD JANUARY 1, 2019 TO DECEMBER 31, 2019
TABLE OF CONTENTS

SECTION 1
Independent Service Auditor’s Report.................................................................3

SECTION 2
Assertion of Algolia, Inc. Management...............................................................6

ATTACHMENT A
Algolia, Inc.’s Description of the Boundaries of Its Search Solution System..................8

ATTACHMENT B
Principal Service Commitments and System Requirements.....................................15
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, 2019 to December 31, 2019, 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).

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.
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, 2019 to December 31, 2019, to provide reasonable assurance that Algolia’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

RESTRICTED USE

Certain 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. Users of this report should have sufficient knowledge and understanding of complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements. Algolia uses multiple data center colocation providers as data center colocation providers. Users of this report should obtain the relevant SOC 2 or SOC 3 reports.

Coalfire Controls LLC

Westminster, Colorado

May 13, 2020
SECTION 2

ASSERTION OF ALGOLIA, INC. MANAGEMENT
Assertion of Algolia, Inc. Management

We are responsible for designing, implementing, operating and maintaining effective controls within Algolia, Inc.’s (“Algolia”) Search Solution System (system) throughout the period January 1, 2019 to December 31, 2019, 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.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2019 to December 31, 2019, 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). 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, 2019 to December 31, 2019, 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 Information Security Management 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 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 together using distributed consensus protocol to ensure consistency of the data and availability of the service. Algolia Search API provides up to 99.999% availability which is achieved by its distributed nature.

In order to mitigate the impact of network latency, Algolia Search API provides an option of enriching 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 having the customer data. Besides lowering network latency, this solution also improves the availability of the whole system by making it more resilient to region scale outages.

Internally, Algolia Search API uses encrypted binary communication protocol between the servers. Externally, Algolia exposes public Hypertext Transfer Protocol (HTTP) and HTTP Secure (HTTPS) interfaces for the 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 Search API. The dashboard also provides user-management functionality.

The Algolia Dashboard is available using HTTPS with 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 & Insight API is a JSON-based API that provides access to analytics data generated from the 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**

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

ALGOLIA SHOPIFY
Algolia Shopify creates a personalized e-commerce site search and discovery experiences that shoppers love.

ALGOLIA CRAWLER (ALGOLIA SITE SEARCH)
Algolia Crawler is a customized site search and discovery tool which automatically extracts and enriches website’s content to deliver it through a rewarding experience. It is a content discovery platform that enables businesses to build, manage and deliver customer centric, content-based experiences on every channel.

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

THE BOUNDARIES OF THE SYSTEM USED TO PROVIDE THE SERVICES
The boundaries of the system are the specific aspects of Algolia’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 system.

The components that directly support the services provided to customers are as 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 (Dallas area), US East (Virginia), Canada (Montreal area), 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 but not limited to OVH, Amazon Web Services (AWS) and Google Cloud Platform.

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. In Algolia’s environment, all the networks are external untrusted and each of the two servers need 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 (located in-house) that supports the infrastructure located at colocation provider facilities.

SOFTWARE
The environment of Algolia heavily utilizes open-source software. Algolia’s environment is composed of multiple systems offering the services to its customers which work in tandem with internal systems supporting the operations of the infrastructure.
Internal Systems

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 exposed 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 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 (CPU), 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 pro-active 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, a local processing of the data is performed, and consistency of the data is verified before further processing. Then an encrypted backup is generated and distributed to the recovery storage closest to the source cluster in order to provide the fastest possible recovery times.

All the databases are backed up once per day using the appropriate database backup mechanisms to ensure 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 on at least an annual basis. System failures that do not impact the availability of the Algolia service are continuously tested to ensure all the 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 the running software are regularly patched. If the particular 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 file integrity and protection of the systems from intrusion. The HIDS performs integrity tests of important files of 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.
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 particular 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 who 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 the feedback from customers, market needs, and future visions of Algolia.

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

Human Resources (HR) of Algolia 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, recovery from failures, administration, and provide an overview of its assets. In order to ease the adoption of internal policies and guide employees through the correct processes, Algolia encompasses as much as possible into internal applications, configuration management, and internal systems.

Algolia has developed policies covering 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 has the ability to trigger critical alerts and notify the 24/7 on-call team in order to resolve immediate issues and restore service. The most critical applications, like Algolia Search API, has the ability to 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.

**DATA**

Algolia’s business does not sell customer data and Algolia has developed an environment that protects the 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”.

**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 public certification authorities. This API follows HTTP standards and is usable as-is or through integration libraries that Algolia provides as an open-source software.

The API features an authentication scheme which 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 proprietary file format, distributed, and stored on Algolia servers composing the solution. All modifications of the data are performed via the API and every interaction with the data is logged. 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/improving of the service.

**Algolia Dashboard**

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

Algolia Monitoring API does not handle customer data. Monitoring API produces data collected from Algolia about the state of the service and makes that information available to customers.

**Algolia Personalization**

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

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

**Algolia Crawler (Algolia Site Search)**

Algolia Crawler is a customized site search and discovery tool which automatically extracts and enriches website’s content to deliver it through a rewarding experience. It is a content discovery platform that enables businesses to build, manage and deliver customer centric, content-based experiences on every channel.

**Logging**

All systems produce application and operations logs which are collected, processed, and stored in Algolia’s systems. These logs are purged from the system following its 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, and thus 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.
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 Master Subscription agreements, Service-level agreements (SLAs), and online in the Company’s Terms of Service and Privacy Policy.

System requirements are specifications regarding how the Algolia Search Solution System should function to meet Algolia’s principal commitments to user entities. System requirements are specified in Algolia’s policies and procedures, which are available to all employees.

Algolia’s principal service commitments and system requirements include the following:

<table>
<thead>
<tr>
<th>Trust Services Category</th>
<th>Service Commitments</th>
<th>System Requirements</th>
</tr>
</thead>
</table>
| 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 and prevention 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.  
  • Algolia will safeguard all confidential information with the same degree of care it would its own information and will not use confidential information other than to provide the Search Solution System. | • Data classification  
  • Retention and destruction standards  
  • Internal confidentiality standards  
  • Information sharing standards |