bright data

# System and Organization Controls Report

# (SOC 3 Report)

# Relevant to Security, Availability, Confidentiality and Privacy

March 1, 2023 – May 31, 2023

# Table of contents

# Section I: Independent Service Auditor's Report

Brightman Almagor Zohar & Co.
1 Azrieli Center, 6701101 P.O.B
16593, Tel Aviv, Israel
Tel: +972 (3) 608 5555
www2.deloitte.com/il/en.html

Deloitte.

# Independent Service Auditor's Report

Bright Data Ltd.

## Scope

We have examined Bright Data Ltd.'s ("Bright Data Ltd.") accompanying assertion titled "Assertion of Bright Data Ltd." (assertion) that the controls related to Bright Data's Data Collector platform were effective throughout the period March 1, 2023 to May 31, 2023 (the "Description"), to provide reasonable assurance that Bright Data's Ltd.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security set forth in TSP section 100, 2017 Trust Services Principles and Criteria for Security, Availability, Confidentiality, and Privacy ("applicable trust services criteria").

## Service Organization's Responsibilities

Bright Data Ltd. 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 Bright Data's Ltd.'s service commitments and system requirements were achieved. Bright Data has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Bright Data 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 on the description and on the suitability of the design and operating effectiveness of the controls stated in the description based on our examination. 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, in all material respects, the description is presented in accordance with the description criteria, and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.
Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Bright Data's service commitments and system requirements based on the applicable trust services.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

## Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA. We applied the statements on quality control standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

## 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 the Service Organization's system were effective throughout the period March 1, 2023 to May 31, 2023, to provide reasonable assurance that Bright Data's Ltd.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

July 23, 2023

# Section II: Management's Assertion

# Assertion of Bright Data Ltd.

We are responsible for designing, implementing, operating and maintaining effective controls over the information systems and technology supporting Bright Data Ltd.'s (the "Service Organization" or "Bright Data") Data Collector platform throughout the period March 1, 2023 to May 31, 2023 to provide reasonable assurance that Bright Data's Ltd.'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 Attachment A below 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 March 1, 2023 to May 31, 2023, to provide reasonable assurance that Bright Data's Ltd.'s service commitments and system requirements were achieved based on the applicable trust services criteria. Bright Data's Ltd.'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 Section IV.

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 March 1, 2023 to May 31, 2023 to provide reasonable assurance that Bright Data's Ltd.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

# Section III: Description of the System

# Section III: Bright Data's Ltd.'s Description of the Boundaries of the Data Collector System

## Bright Data Ltd. Business Overview

Bright Data is a web data platform, founded in 2014, which provides all types of companies' solutions to retrieve crucial public web data in the most efficient, reliable, and flexible way. Using web data, companies can research, monitor, and analyze required data to make better business decisions.

Bright Data's platform is used by 15,000+ customers worldwide in nearly every industry.

## Services Provided

**Web Scraper IDE**

Bright Data collects web data at scale with zero infrastructure using one of hundreds of ready-made Web Scraper IDE templates targeting popular websites.

AI algorithms seamlessly clean, match, synthesize, process, and structure the unstructured website data before delivery – resulting in datasets ready for analysis.

Web Scraper IDE is layered over the company's industry-leading, patented, peer-network technology, with the ability to tap into difficult-to-access public websites.

**Datasets**

Bright Data's Datasets cover data points from e-commerce, social media, jobs & other popular websites.

Bright Data identifies and analyzes trends, finds companies, people, and social media influencers, to optimize its user's e-commerce activity, or obtain data for the customer's machine learning algorithms.

Bright Data can also customize an existing dataset based on location, category, or any other parameter using our smart filtering capabilities.

## Control Environment Area

The control environment at Bright Data is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. It reflects the overall attitude, actions of management and others concerning the importance of controls and the emphasis given to controls in Bright Data's policies, procedures, methods and organizational structure. The Key elements of Bright Data's control environment includes Oversight by Bright Data's Board of Directors, HR Policies and practices and integrity and ethical values.

## Organization and Management

Bright Data's Management team has the responsibility to manage Bright Data and its business on a daily basis.

The management assigns authority and responsibility for operating activities and establishes reporting

relationships and authorization hierarchies. In addition, the management has responsibility for design policies and communications so that personnel understand Bright Data's objectives.

- Bright Data’s Management team is responsible for approving the information security policies and procedures and overview implementation.
- Approving and monitoring the information security annual activity program.
- Approving information classification levels and setting the required security level for relevant systems.
- Bright Data’s security steering committee communicates on a monthly basis.
- The Information security steering committee shall convene at least once a year for a formal information security overview.

### People

Bright Data assures that every employee of the company and third-party employees are suitable for the position intended to them and understand the responsibilities imposed on them, in order to prevent events of failure, fraud or abuse of information and assets of either the company and/or its customers.

Each employee shall sign a confidentiality agreement and a code of conduct, whereby he will maintain the rules of information security and privacy, as a condition of his work with the company.

### Integrity and ethical values

Integrity and ethical values are essential elements of the control environment.

Bright Data's code of conduct is a set of company values, rules, and includes principles for outlining the behavioral expectations within Bright Data.

- All employees are required to read and accept the code of conduct as part of Bright Data’s onboarding process.
- Bright Data's policies include probation, suspension, and termination as potential consequences of employee misconduct.

### Communication and Information

An Information Security Policy is in place addressing system requirements for all users. The policy is reviewed and updated on an annual basis and as needed by the Chief Technology Officer.

Associates have access to security policies. Bright Data published its IT security policies on its internal drive.

### Risk Assessment

- The Internal Audit function conducts a yearly risk assessment. The risk assessment is used to drive the activities of the internal audit function.
- Key finance personnel hold periodic meetings among executive management, IT personnel, and legal counsel to identify issues that may affect relevant trust principles.
- The functions in the company that are in charge with governance hold periodic reviews of Bright Data’s compensation and performance evaluation programs to identify potential incentives and pressures for

employees to commit fraud.

### Monitoring

- Bright Data has deployed firewalls and rule configurations to protect Bright Data's servers against outsiders and threats to the system's security. Firewall consoles are monitored by the Infosec (Information Security) Team and unusual activity noted is researched and resolved.
- The organization periodically assesses the sufficiency of its information systems to capture and report data that are timely, current, accurate, and accessible.
- For high severity incidents, Root Cause Analysis (RCA) is performed through various tools and meetings in order to improve the quality Bright Data's provided services.
- SLA with third parties exist and includes monitoring the process and the access (As applicable).
- Management assesses the risks associated with subservices organizations and has implemented various management oversight and monitoring processes to confirm that the subservice organizations continue to provide services in a controlled manner.

### Internal Audit

Bright Data established internal audit procedures and techniques as part of the company's Risk- Management implementation.

Each department manager is required to hold an internal audit for the processes and procedures in his field at least once a year. Audit procedures steps are:

(1) Assess current processes and procedures.
(2) Analyze and compare results against internal control objectives to determine whether audit results comply with internal policies and procedures as well as federal and state rules and regulations.
(3) Compile an audit report to present to the business owner.

### Incident Management

Bright Data's Incident Response procedure addresses the means necessary to ensure effective response to incident relevant to the system, identifying the lifecycle of the incident management, including the incident identification, investigation, prioritization and mitigation.
Every employee of Bright Data, suspecting an Information security incident must report it to the Information security team. The security team is responsible for carrying out an initial examination of any suspected IS incident, and to commence with the treatment process, in collaboration with the relevant professional bodies pursuant to the treatment of the incident.

### Availability

### Backup and Monitoring

- All necessary data for the workloads Bright Data's used servers are running. This may include documents, media files, configuration files, operating systems, registry files, etc.
- Bright data shall use cloud storage technologies to allow automatic data recovery.
- A Large-scaled overall disaster recovery drill will take place on a yearly basis.

- Backup copies are made on a consistent, regular basis to minimize the amount of data lost between backups.
- Bright Data has a Data Retention Policy, stating that data will be retained for as long as required by applicable laws and according to the retention period set within contracts.
- Retaining multiple copies of data provides the insurance and flexibility to restore to a point in time not affected by data corruption or malicious attacks.
- Bright Data configures full, daily database backups for all data stored for our company by AWS cloud storage services.
- Bright Data stores all its business data, including customers data, on cloud service provider's servers.
- Bright Data uses AWS Backup to create daily backups, snapshots are kept monthly. The snapshots are encrypted.

### Change Management

Bright Data has formal change management procedures for infrastructure (e.g., firewall rules, AWS configurations, etc.) and application changes to help ensure that all changes are reviewed, approved, tested, and logged. These procedures describe the key steps within the change management process, such as change requests, approvals, planning, notifications to affected parties, testing results, rollbacks, and steps to be taken to implement planned and emergency changes.

Required changes are defined by Bright Data's Product team, creating a 'Definition of Done' (DoD) document which is also approved by VP Product.

The DoD will be reviewed by the R&D team, ensuring deliverables and dependencies for execution are acceptable, including an analysis of all relevant requirements, resources, and timelines. All changes requirements are categorized according to urgency.

During the R&D review, proposed changes are evaluated to determine if they present a security risk and what mitigating actions will be required.

Once a change project is developed, the R&D team will also create an automated testing process, as well as a deploy procedure for the Deploy team to follow.

### Risk Mitigation

### Vendor risk management

- All vendors in Bright Data should be mapped and categorized, following a risk assessment.
- Suppliers shall be classified into three levels that indicate their level of risk for the organization.
- The information security team shall be informed by the procurement team regarding proposed contractual agreements with high-risk suppliers to initiate the risk assessment following a security questionnaire.

- The information security team will be responsible for carrying out the risk assessment with the relevant suppliers prior to the signing of the contract.
    (1) Since Bright Data is obligated to comply with legal and regulatory requirements, the suppliers providing services to Bright Data by default must comply with the same requirements.

### Privacy

Bright Data has gone through a comprehensive GDPR and CCPA compliance program and has implemented the necessary measures and procedures for the safeguard of our customers' personal data. As part of such program, Bright Data is following the GDPR / CCPA requirements and best practice industry standards with respect to any aspect of its business that may affect personal data, including but not limited to: information security, transfer of personal data outside of the EEA, the exercise of data subjects' rights, assistance to controllers, employees' training, use of third-party service providers including share of personal information, retention and deletion of personal data. It is important to emphasize that Bright Data has no control over the personal data, types of personal data that is being uploaded to its platform and does not further classify Customer Data.

Data privacy impact assessments are being conducted as part of the Product flows in order to verify that indeed data is being collected according to Bright Data's requirements and obligations.

Bright Data Privacy policy is updated and reviewed on an annual basis and is publicly available at https://BrightData.com/privacy.

# Section IV: Principal Service Commitments and System Requirements

Bright Data makes service commitments to its customers, business partners, and vendors, and has established system requirements as part of the Data Collector service. Some of these commitments are principal to the performance of the service and relate to applicable trust services criteria. Bright Data 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 Bright Data's service commitments and system requirements are achieved.

The Service Organization's security commitments in regard to the systems and operations are also documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided to user entities. Those objectives are based on the service commitments that Bright Data makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that Bright Data has established for the services.

Service commitments are standardized and include, but are not limited to, the following:

**Security**: Bright Data has made commitments related to securing customer data and complying with relevant laws and regulations. These commitments are addressed through measures including data encryption, authentication mechanisms, physical security and other relevant security controls.

**Availability**: Bright Data has made commitments related to percentage uptime for instances of downtime.

**Confidentiality**: Bright Data has made commitments related to maintaining the confidentiality of customers' data through data classification policies, data encryption and other relevant security controls.

**Privacy**: Bright Data has made commitments related to maintaining the Personal Identifiable Information of customers through data privacy policies, retention and disposal and other relevant security and privacy controls.

Bright Data establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements.

Such requirements are communicated in Bright Data's systems policies and procedures, system design documentations, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how systems are operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of relevant services provided to its customers.