

*Audit Report for the period of
April 1, 2024, to May 31, 2025*

ISAE 3000 Type II Compliance and Ethics Control Assurance Report

**Report on the control environment for
compliance and ethics and on the matter of the
design and operating effectiveness**

Table of Contents

1. PwC Report of Independent Service Auditors	3
1.1. Scope	3
1.2. Bright Data's Responsibilities	3
1.3. Our Independence and Quality Control	3
1.4. Service Auditor's Responsibilities	3
1.5. Opinion	3
1.6. Limitations	3
1.7. Intended Use and Purpose	4
2. Bright Data's Assertion and Service Description	5
2.1. Introduction	5
2.2. Bright Data's Services, Systems and Infrastructure	5
2.3. Compliance and Ethics Control Environment	6
3. Compliance and Ethics Control Objectives, Related Controls, Review and Testing of Design and Operating Effectiveness	9
3.1. Methodology	9
3.2. Control Group #1 – Policies	9
3.3. Control Group #2 – Domain Restrictions	11
3.4. Control Group #3 – Network Restrictions	12
3.5. Control Group #4 – Health Monitoring	15
3.6. Control Group #5 – Abuse Reporting	15
3.7. Control Group #6 – SDK Restrictions	16
3.8. Control Group #7 – Dataset Inspection	17
3.9. Control Group #8 – Training	19

1. PwC Report of Independent Service Auditors

1.1. Scope

PricewaterhouseCoopers Digital Technology Services LTD (PwC Digital Technology Services LTD), a subsidiary of PricewaterhouseCoopers Israel (PwC Israel), have been engaged to report on Bright Data's control environment for compliance and ethics for its services, systems and infrastructure as described in Chapter 2. This assessment is for the period of April 1, 2024, to March 31, 2025.

1.2. Bright Data's Responsibilities

Bright Data is responsible for preparing the description of its services, systems and infrastructure, and compliance and ethics controls in chapter 2. This includes responsibility for the completeness, accuracy and method of presentation, providing the services covered by the description, stating the control objectives, and effectively designing, implementing and operating controls to achieve the stated control objectives.

1.3. Our Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants. This is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

1.4. Service Auditor's Responsibilities

Our responsibility is to express an opinion on Bright Data's control environment for compliance and ethics and their design, in relation to the control objectives stated, and the operating effectiveness. We conducted our engagement in accordance with International Standard on Assurance Engagements 3000 Type II issued by the International Auditing and Assurance Standards Board. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operated, to achieve the stated control objectives. We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

1.5. Opinion

Our opinion has been formed based on the matters outlined in Chapter 3 in this report. In our opinion, in all material respects, the controls tested are designed and operated effectively throughout the period from April 1, 2024, to March 31, 2025.

1.6. Limitations


Bright Data's description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment.

1.7. Intended Use and Purpose

This report is intended for customers who have used, or will potentially use, Bright Data's service deliveries, and their auditors, who have a sufficient understanding to consider it.

Tel-Aviv, June 29th, 2025

PwC Digital Technology Services Ltd
מי.דאבליו.סי שירותי טכנולוגיות דיגיטל בע"מ

A handwritten signature in black ink that reads 'Talya Gazit'.

Talya Gazit, CEO

PwC Digital Technology Services LTD

2. Bright Data's Assertion and Service Description

2.1. Introduction

2.1.1. About Bright Data

Bright Data is the DaaS leader in web data, trusted globally by over 20,000 customers as critical infrastructure for AI, finance, e-commerce, travel, marketing, and other sectors. Bright Data's unmatched scale, compliance, and reliability, supports every data-collection workflow - from DIY scraping to fully automated delivery.

2.1.2. Web Scraping and Ethical Considerations

Web scraping is the automated process of extracting information from websites. It involves using dedicated software to simulate human browsing behavior, such as loading web pages, navigating links, and copying data, so that the desired content can be collected, structured, and stored for later use. Common use cases include critical infrastructure for AI, price comparison by scraping product and real estate listings, market research analysis by collecting product reviews, news and trends monitoring and narrative analysis by gathering news headlines and articles, and enriching business development and lead generation by collecting company data and business emails.

Web scraping should be performed ethically to ensure the protection of users, network, and the world wide web, while complying with relevant regulations. Measures to ensure ethical web scraping and data collection can include accessing public web data only (data that is not behind login mechanisms or paywalls), preventing overloading servers with high-frequency requests (DDoS), and ensuring transparent and ethical network sourcing.

Bright Data's services and tools assist in accessing public web data while ensuring ethical usage to all.

2.2. Bright Data's Services, Systems and Infrastructure

2.2.1. Proxy Services

Bright Data offers a range of proxy services designed to enable ethical and large-scale data collection from the web. A proxy acts as an intermediary between a user and the internet, allowing the user to send web requests through a different IP address as though they are coming from another location or identity. Bright Data offers two main proxy types:

- Static – These include IP addresses issued by Internet Service Providers ("ISP") or Data Centers ("DC") and acquired by Bright Data.
- Rotating – These include Residential and Mobile IP addresses which are sourced from real users who have opted in to Bright Data's network and are sharing their network resources.

2.2.2. Data Extraction Tools

Bright Data's Data Extraction Tools are based on Bright Data's proxy infrastructure and are designed to help businesses programmatically access public web data reliably. These APIs abstract away the complexity of managing proxies, browser behavior, and anti-bot mechanisms, allowing developers and organizations to focus on data extraction. The tools provide a simple and unified interface to fetch web data by routing requests through Bright Data's proxy infrastructure, with options for browser emulation, JavaScript rendering, etc. Main Data Extraction Tools are:

- **Web Unlocker** – The Web Unlocker API is designed to allow web access. It handles JavaScript rendering, CAPTCHAs, session management, and IP rotation.
- **SERP (Search Engine Results Page) API** – The SERP API is purpose-built for retrieving structured search engine results from platforms like Google and Bing. It supports, among others, localized queries, ads, shopping results, and returns clean JSON output.
- **Browser API** – The Browser API gives access to a full real-time browser, operating over the proxy network. It is emulating human interaction with websites, rendering JavaScript, and using real browser fingerprints.

2.2.3. Datasets

Bright Data offers a wide range of pre-collected and custom web datasets, providing structured, reliable, and up-to-date public web data for businesses and researchers. These datasets help companies gain insights, fuel AI models, perform competitive analysis, and make data-driven decisions.

2.2.4. Software Development Kit

Bright Data's Software Development Kit (SDK) is a lightweight and embeddable module that app developers can integrate into their applications to enable opt-in proxy participation in Bright Data's rotating proxy network. It allows developers to monetize their apps by enabling users to consensually share their device's IP address and network resources.

2.3. Compliance and Ethics Control Environment

Bright Data operates with a strong and transparent Compliance and Ethics Control Environment, which is designed to ensure that its powerful data collection technologies are used responsibly and ethically. As the world's leading public web data platform, Bright Data prioritizes compliance, user protection, and accountability, setting industry standards for ethical web scraping and proxy infrastructure management. Bright Data's Ethics and Compliance Environment exists to ensure that all data access and usage complies with applicable laws, data is collected and processed in a socially responsible way, and that Bright Data's platform is not misused for malicious, abusive, or exploitative purposes. Core principles of the environment are proactive abuse prevention and ethical use case enforcement.

2.3.1. Policies

Bright Data's Acceptable Use Policy (AUP) is part of Bright Data's license agreement and a critical framework that governs how its data collection and proxy services can be used. The AUP is designed to ensure that customers operate within the bounds of the law, respect third-party rights, and uphold global compliance, ethical, and regulatory standards. Bright Data's AUP defines what is and is not permitted when using its services, the types of targets, content, and data collection behaviors that are prohibited, and the legal and regulatory compliance obligations of the customer. It applies to all users of Bright Data's platform.

2.3.2. Domains Restrictions

Bright Data implements strict domain-level restrictions to uphold its ethical standards, and protect its customers, network and the world wide web. It maintains blacklists and controlled access lists of websites that cannot be scraped using its platform, either by default or without explicit approval.

While some of the domain restrictions are aimed at protecting potentially high-risk domains like governmental websites, other restrictions are set to prevent the misuse of Bright Data's network for unapproved use cases such as Gambling and Adult content.

2.3.3. Network Restrictions

To prevent misuse of its powerful web data collection tools, Bright Data prevents their use on non-default HTTP-related ports and protocols. In addition, its Browser API service is not allowed to perform authentication attempts to websites. To be granted an exception to the above, a user must undergo a rigorous Know Your Customer (KYC) process, which includes business validation, contact verification, and approval of the intended use case.

2.3.4. Health Monitoring

Bright Data's platform includes robust website health monitoring capabilities as part of its data collection and ecosystem. The capabilities are designed to track, analyze, and maintain the availability of public web data sources. It verifies that a target website is online and reachable and monitors the domain responsiveness to identify performance issues. If an interruption is detected, traffic originating from Bright Data's platform is automatically throttled and rate-limited automatically.

2.3.5. Web Master Console

Bright Data's Webmaster Console is a unique feature designed specifically for website owners and operators who want visibility, control, and consent management over how their websites are accessed by Bright Data's data collection infrastructure. It reflects Bright Data's commitment to transparency and ethical data collection by empowering webmasters to monitor, restrict, or customize how their sites are being accessed through Bright Data's services. The Webmaster Console is a self-service portal that allows website owners to inspect traffic coming from Bright Data's proxy networks and control how their site is accessed.

2.3.6. Abuse

Bright Data provides dedicated abuse reporting channels as part of its strong commitment to legal compliance, ethical data collection, and protection of third-party rights. These channels allow website owners, users, regulators, or the public to report violations or concerns related to Bright Data's infrastructure, customers, or data collection activities. Abuse refers to any alleged unauthorized, unethical, or unlawful use of Bright Data's proxy networks, data collection tools, or scraping platforms, such as unauthorized data access, website performance degradation, spam or fraudulent activity, and domain restrictions violations.

Bright Data's abuse reporting channels include an online abuse reporting form (<https://brightdata.com/report-abuse>) and email reporting (to abuse@brightdata.com). Bright Data's Compliance and Ethics Team investigates all reports while ensuring timely response, confidential handling, and cooperation with law enforcement and regulators in case of criminal misuse.

2.3.7. Software Development Kit (SDK)

Embedding and integrating Bright Data's SDK into an application requires a thorough review and subsequent approval by Bright Data to ensure alignment with its compliance and ethical standards. Every user of an integrated application must consensually opt-in and provide his informed consent to be included in Bright Data's rotating proxy network and share his device's IP address.

2.3.8. Datasets

Bright Data's pre-collected datasets may contain personal identifiable information (PII). For maintaining compliance with data protection standards, Bright Data developed suitable administrative and technical controls to comply with relevant privacy regulation and allow data subjects to exercise their privacy rights.

2.3.9. Training

Bright Data's Compliance and Ethics Team developed a yearly compliance and ethics internal online training for the company employees. This is a preventive control for educating its employees regarding the organizational standards of compliance and ethics and other related laws and regulations. The training is aimed at educating all relevant departments in Bright Data regarding ethical proxy and data collection use.

3. Compliance and Ethics Control Objectives, Related Controls, Review and Testing of Design and Operating Effectiveness

3.1. Methodology

The compliance and ethics control environment represents the collective of controls, their design, development and operation, and the effect of it for preventing and mitigating compliance and ethics issues according to Bright Data's compliance and ethics policy and objectives. Review and tests of the control environment included the following methods, to the extent we considered necessary:

1. Reviews of Bright Data's organizational structure, including policy statements and policies.
2. Review of the design of compliance and ethics procedures performed by Bright Data's Compliance and Ethics Team.
3. Review of the operating effectiveness of compliance and ethics procedures performed by Bright Data's Compliance and Ethics Team by sampling and reviewing procedures executed.
4. Review of the design of compliance and ethics controls implemented by Bright Data.
5. Review of the operational effectiveness of compliance and ethics controls implemented by Bright Data.
6. Discussions with management, operations, administrative, and other personnel who are responsible for designing, developing, applying and operating controls.

3.2. Control Group #1 – Policies

Control Group Objective		
Set and enforce ethical use of Bright Data's services and products.		
Control Description	Review and Testing Activities	Review and Testing Results
Bright Data's "Acceptable use policy" represents the company standards regarding ethical use of its services and products and is reviewed by Bright Data's "Data Ethics Committee" on a yearly basis.	Review of Bright Data's Acceptable Use Policy.	By reviewing Bright Data's Acceptable Use Policy provided publicly on its website, we can conclude it provides a comprehensive framework that prohibits common proxy abuse scenarios.

Control Description	Review and Testing Activities	Review and Testing Results
	Review of Bright Data's Data Ethics Committee.	Per a formal management announcement by the Chief Compliance and Ethics Officer for the establishment of the company Data Ethics Committee, we can verify the Data Ethics Committee was established in January 2024. It is responsible for developing and implementing a data risk framework, which will define the guiding principles, policies, standards, and controls for data ethics in all Bright Data's products and services. It is composed of executive management from different functions and departments.
	Review of evidence of yearly reviewal and approval of the Acceptable Use Policy by the Data Ethics Committee of Bright Data.	Evidence of review and approval of the Acceptable Use Policy by the Data Ethics Committee of Bright Data for 2024 was presented.
Customers with unapproved use cases, as described in Bright Data's "Acceptable Use Policy", are denied from using Bright Data systems and products.	Review of policy enforcement processes as managed by Bright Data.	Bright Data's policy enforcement is verified both as part of the service Terms and Conditions which refers to Bright Data's Acceptable Use Policy, and is approved by any new user, and by reviewing evidence of unapproved use cases requests decline and account disabling if any unethical usage is requested, reported or detected.

3.3. Control Group #2 – Domain Restrictions

Control Group Objective		
Block restricted web content according to Bright Data's Acceptable Use Policy.		
Control Description	Review and Testing Activities	Review and Testing Results
Bright Data blocks certain web content according to a domain classification system. This includes adult content, governmental websites, harmful domains, gambling, and other potential high-risk domains, as determined by Bright Data.	Review of Bright Data's domain classification scheme.	By reviewing Bright Data's domain classification scheme, we can conclude it is comprehensive and clear. It is implemented at the rotating proxy infrastructure level.
	Review the technical block access mechanism according to the domain classification scheme.	Bright Data's domain classification scheme for access detection and block is effectively implemented within its infrastructure. Therefore, we can conclude Bright Data's domain classification scheme is effectively designed.
	Perform access attempts to restricted domains using a service of Bright Data.	Access attempts to block classification websites were performed using Bright Data's service. Those access attempts were successfully blocked. Therefore, we can conclude Bright Data's domain classification scheme is effectively operated.
Bright Data blocks governmental domains (*.gov) across all proxy networks.	Review the mechanism by which Bright Data blocks government domains.	Bright Data's infrastructure is verified for containing a mechanism by which gov top-level domain, that is used by government websites, cannot be accessed by Bright Data's infrastructure. This verification took place by reviewing the source code that operates this mechanism. Therefore, we can conclude Bright Data's mechanism for blocking government domains is effectively designed.

Control Description	Review and Testing Activities	Review and Testing Results
	Perform access attempts to governmental domains using a service of Bright Data.	Access attempts to governmental websites were performed using different Bright Data services. Those access attempts were successfully blocked. Therefore, we can conclude Bright Data's mechanism for blocking government domains is effectively operated.

3.4. Control Group #3 – Network Restrictions

Control Group Objective		
Access to advanced and/or restricted features of Bright Data require a dedicated review process for preventing unethical use.		
Control Description	Review and Testing Activities	Review and Testing Results
Access to Bright Data's rotating proxy network is subject to a "Know Your Customer" ("KYC") review process, which includes a detailed identity verification and use case review.	Review the mechanism by which every access to Bright Data's rotating proxy network is subject to a Know Your Customer (KYC) review process.	Per our review, we can conclude that every access to Bright Data's rotating proxy network is subject to a Know Your Customer (KYC) review process by effective administrative and technical mechanisms. Therefore, we can conclude it is effectively designed.
	Check whether every Know Your Customer (KYC) process includes a detailed identity verification and use case review, as stated.	A sample of Know Your Customer (KYC) processes was reviewed. They included detailed identity verification and use case review. Therefore, we can conclude it is effectively operated.

Control Description	Review and Testing Activities	Review and Testing Results
Use of non-default protocols and ports (other than http:80 and https:443) across all Bright Data's services is subject to a "Know Your Customer" ("KYC") review process, which includes a detailed identity verification and use case review.	Review the mechanism by which every use of non-default protocols and ports is subject to a Know Your Customer (KYC) review process.	Using non-default protocols and ports across all Bright Data's services is subject to a Know Your Customer (KYC) review process by an effective administrative procedure performed by Compliance and Ethics Team. An unauthorized use of non-default protocol or port is blocked by default across all Bright Data's services by a technical mechanism implemented by the source code of Bright Data's infrastructure.
	Perform unauthorized access attempts to a non-default protocols and ports.	Unauthorized access attempts to a non-default protocols and ports were performed. Those access attempts were successfully blocked.
User login access (using username and password) is blocked by default in Bright Data's Browser API product to prevent access to non-public data.	Review the mechanism by which user login attempts are blocked by Browser API.	User login access is blocked by default in Bright Data's Browser API by a technical mechanism implemented by its source code.
	Perform unauthorized user login attempts using Browser API.	User login attempts were performed using Bright Data's Browser API. Those access attempts were successfully blocked.

Control Description	Review and Testing Activities	Review and Testing Results
Domain owners can view the traffic sourced from Bright Data's products and manage access to sensitive end points and non-public information, by implementing Bright Data's <i>collectors.txt</i> data collection protocol.	Review the mechanism by which domain owners can monitor traffic originated from Bright Data and manage it for applying restrictions.	Bright Data offers its Web Master Console for domain owners for monitoring traffic originated from the Bright Data Network. It allows them to implement a <i>collectors.txt</i> file and control over scraping activity, including blocking non-public and sensitive end points, classify data as including PII and configure general scraping activity. Bright Data's infrastructure is verified for containing a mechanism by which a <i>collectors.txt</i> file of a domain name is read, parsed and followed by Bright Data's infrastructure. This verification took place by reviewing the source code that operates this mechanism. Therefore, we can conclude this mechanism is effectively designed.
	Use Bright Data's Web Master Console for a demo domain for traffic monitoring and for applying and testing restrictions implemented by a <i>collectors.txt</i> file.	Web Master Console was verified as specific inbound traffic to a demo website originated from the Bright Data Network was observed and monitored. As part of it, restrictions were applied by implementing a <i>collectors.txt</i> file. They were tested by performing access attempts to restricted resources, which were blocked successfully. Therefore, we can conclude this mechanism is effectively operated.

3.5. Control Group #4 – Health Monitoring

Control Group Objective		
Bright Data must not cause an interruption or outage to websites or APIs.		
Control Description	Review and Testing Activities	Review and Testing Results
Automatic domain responsiveness monitoring systems are in place to prevent domain degradation.	Review the mechanism and monitoring systems by which domain responsiveness is monitored.	Bright Data monitors the responsiveness of domains using a proprietary monitoring mechanism within its infrastructure. This monitoring mechanism throttles traffic originated from Bright Data's infrastructure upon detection of degradation in the responsiveness of a domain in real-time. According to our review, it is designed effectively.
	Review the mechanism by which traffic originated by Bright Data is throttled as a response to degradation in the responsiveness of a domain.	
	Review a sample of cases where the monitoring system detected possible abnormalities and executed automatic mitigation.	A sample of cases where the monitoring system detected possible abnormalities was reviewed. In all of them, an efficient detection and mitigation was performed. Therefore, we can conclude it is operated effectively.

3.6. Control Group #5 – Abuse Reporting

Control Group Objective		
Bright Data is responsible for addressing and mitigating potential abuse activity reported by affected entities.		
Control Description	Review and Testing Activities	Review and Testing Results
All Bright Data's abuse and suspicious activity reporting channels are monitored and reviewed manually to ensure use of its network in accordance with Bright Data's standards.	Review Bright Data's abuse and suspicious activity reporting channels.	According to our methodological review, Bright Data's abuse and suspicious activity reporting channels are designed effectively.
	Review the monitoring and review processes Bright Data performs upon an abuse and suspicious activity reporting.	Monitoring and review processes performed by Bright Data upon an abuse and suspicious activity reporting are managed and operating effectively for addressing issues in a timely and a completed manner.

Control Description	Review and Testing Activities	Review and Testing Results
	Review a sample of abuse and suspicious activity reporting tickets to verify they were handled in alignment with Bright Data's standard and corresponding procedure.	A sample of abuse and suspicious activity reports were reviewed, and it can be concluded that the monitoring and review process is operated effectively.

3.7. Control Group #6 – SDK Restrictions

Control Group Objective		
Usage of Bright Data's SDK requires a dedicated review process for preventing unethical use, and ensure users provide their consent.		
Control Description	Review and Testing Activities	Review and Testing Results
Every implementation of Bright Data's Software Development Kit ("SDK") in applications is reviewed to ensure alignment to Bright Data standards.	Review the approval process performed by Bright Data for approving or rejecting a request to implement its SDK in an application, including the review of the obligatory opt-in and opt-out mechanism and the information presented to the user upon opting in.	Bright Data's review process performed by Bright Data for approving or rejecting a request to implement its SDK in an application, includes the review of the obligatory opt-in and opt-out mechanism and the information presented to the user upon opting in, and is designed effectively.
	Review the mechanism by which only approved applications can use Bright Data's SDK.	A technical mechanism implemented in the source code of Bright Data's infrastructure is set so only approved applications can utilize Bright Data's SDK.
	Review a sample of applications in which Bright Data's SDK was implemented to verify they were handled in alignment with Bright Data's standard and corresponding procedure.	A sample of approved applications and their review processes were reviewed, and it can be concluded that the review process is operated effectively.

Control Description	Review and Testing Activities	Review and Testing Results
To be included in the Bright Data rotating network and allow the use of the user IP, the user must actively opt-in within the application and allow access and usage.	Review the opt-in process taken by a user to be included in the Bright Data rotating network and allow the use of its IP and the list of IPs included in the rotating network, and ensure only opt-in users are included in the rotating network and no automatic or default opt-in mechanism is in place.	Bright Data's opt-in process is mandatory for a user to be included in the Bright Data rotating network and allow the use of its IP, and only opt-in IPs are included in Bright Data's rotating IP network list of IPs.
	Review the code and default block mechanism by which an IP address can only be included in Bright Data's rotating network, if the associated user has opted in.	According to reviewing Bright Data infrastructure, an IP address of a user that was not opted will never be part of Bright Data's rotating network.
	Review a sample of IPs included in Bright Data rotating network and verify they are opted in.	A sample of IPs included in Bright Data rotating network was reviewed, and it was verified that the associated user was opted in.
As part of the opt-in process to Bright Data's rotating network, the user is informed of the following: [1] General intended use of the IP address by Bright Data [2] Limited access to the IP by Bright Data only [3] Information about Bright Data [4] Opt-out option [5] Link to Bright Data privacy policy [6] Link to Bright Data End User License Agreement.	Review the information provided to a user upon opting in to Bright Data's rotating network.	According to the audit procedures performed, the mentioned information is presented to every user as part of their opt-in process in an app.

3.8. Control Group #7 – Dataset Inspection

Bright Data grants data subjects the control over their personal data in alignment with data protection laws and regulations.		
Control Group Objective		
Control Description	Review and Testing Activities	Review and Testing Results
Bright Data datasets that are published in Bright Data's dataset market are reviewed and approved by Compliance and Legal.	Review the review and approval process of the datasets prior to publication.	Bright Data's review and approval process performed by Bright Data prior to publication is designed effectively by Compliance and Legal for being aligned with Bright Data's internal standards.
	Review a sample of the datasets and their review and approval processes to verify they were handled in alignment with Bright Data's standard and corresponding procedure.	A sample of datasets and their review and approval processes were reviewed, and it can be concluded that the process is operated effectively.
Notifications are sent to identified data subjects via email, allowing them to exercise their privacy rights.	Review the mechanism by which data subjects for which personal information is collected are identified and notified.	Bright Data's infrastructure was verified to include a mechanism that identifies a data subject's email address during public data collection and automatically sends them a notification informing them of the data collection, and their privacy rights. This verification took place by reviewing the source code that operates the mechanism.

Control Description	Review and Testing Activities	Review and Testing Results
Following the processing of a data subject request to delete their data and/or opt-out from Bright Data's data sets data collection process, Bright Data takes actions to prevent further data regarding such data subjects from being collected.	Review the mechanism by which personal information collection is avoided for a data subject that requested Bright Data to delete their personal information from Bright Data's datasets and/or requested to opt-out from Bright Data's services.	Bright Data's infrastructure is verified for containing a mechanism by which personal information is avoided from being collected for a data subject that requested Bright Data to delete their personal information from Bright Data's datasets and/or requested to opt-out from Bright Data's services. This verification took place by reviewing the technical pipeline and source code that operates this mechanism.

3.9. Control Group #8 – Training

Control Group Objective		
Bright Data ensures its employees understand and adhere to the organizational standards regarding compliance and ethics and other related laws and regulations.		
Control Description	Review and Testing Activities	Review and Testing Results
Company employees are required to complete a yearly cross company compliance and data ethics training.	Review Bright Data's Compliance and Data Ethics Training and its contents.	<p>Bright Data's Compliance and Data Ethics yearly training was developed and is updated by the Compliance and Ethics Team. The 2024 cross-company training campaign was launched in November 2024 and employees' participation was monitored in the company's learning management system.</p> <p>By reviewing its contents, we can conclude Bright Data's Compliance and Data Ethics Training is designed effectively to educate its employees regarding the organizational standards regarding compliance and ethics and other related laws.</p>

Control Description	Review and Testing Activities	Review and Testing Results
	Review evidence shows all employees complete this training on a yearly basis.	According to the company's LMS, all Bright Data employees completed the training for this audit period.