Dreamdata®

System and Organization Controls (SOC) 3

Relevant to the Trust Service Criteria for Security

For the Period
March 20, 2025 to March 20, 2026

JOHANSON GROUP

johansonllp.com

Table of Contents

I.	**Independent Service Auditor's Report**	**3**
II.	**Assertion of Dreamdata.io ApS Management**	**5**
III.	**Description of The Dreamdata Platform**	**9**



Section I
Independent Service Auditor's Report

I. Independent Service Auditor's Report

Dreamdata.io ApS

Scope

We have examined Dreamdata.io ApS Dreamdata.io ApS's accompanying description of its The Dreamdata Platform (system) titled "Description of The Dreamdata Platform" throughout the period March 20, 2025 to March 20, 2026 (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period March 20, 2025 to March 20, 2026, to provide reasonable assurance that Dreamdata.io ApS Dreamdata.io ApS's service commitments and system requirements were achieved based on trust services criteria relevant to security principles (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

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

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

Service Organization's Responsibilities

Dreamdata.io ApS 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 's service commitments and system requirements were achieved. Dreamdata.io ApS has provided an assertion titled "Assertion of Dreamdata.io ApS's Management" (assertion) about the description and the suitability of the design and operating effectiveness of the controls stated therein. Dreamdata.io ApS is responsible for preparing the description and assertion; including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria, and stating the related controls in the description, and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

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 controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. 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 operated 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.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- 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 the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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

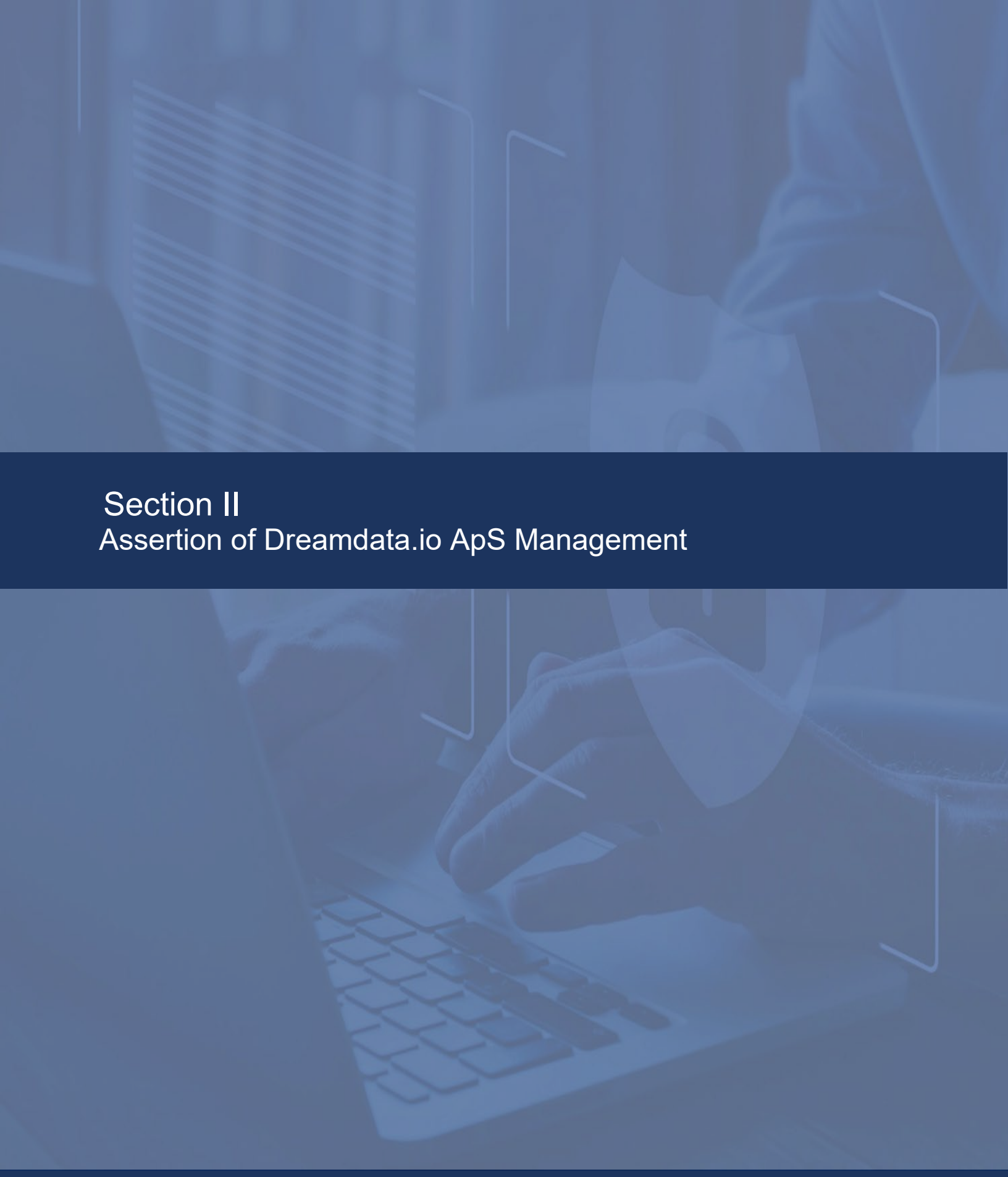
Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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 Dreamdata.io ApS Dreamdata.io ApS'sThe Dreamdata Platform (system) were effective throughout the period March 20, 2025 to March 20, 2026, to provide reasonable assurance that Dreamdata.io ApS service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

JohansonGroup LLP

Colorado Springs, Colorado
April 30, 2026



Section II
Assertion of Dreamdata.io ApS Management

II. Assertion of Dreamdata.io ApS Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Dreamdata.io ApS Dreamdata.io ApS's The Dreamdata Platform (system) throughout the period March 20, 2025 to March 20, 2026, to provide reasonable assurance that Dreamdata.io ApS Dreamdata.io ApS's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in the section of this report titled, “Description of The Dreamdata Platform” and identifies the aspects of the system covered by our assertion.

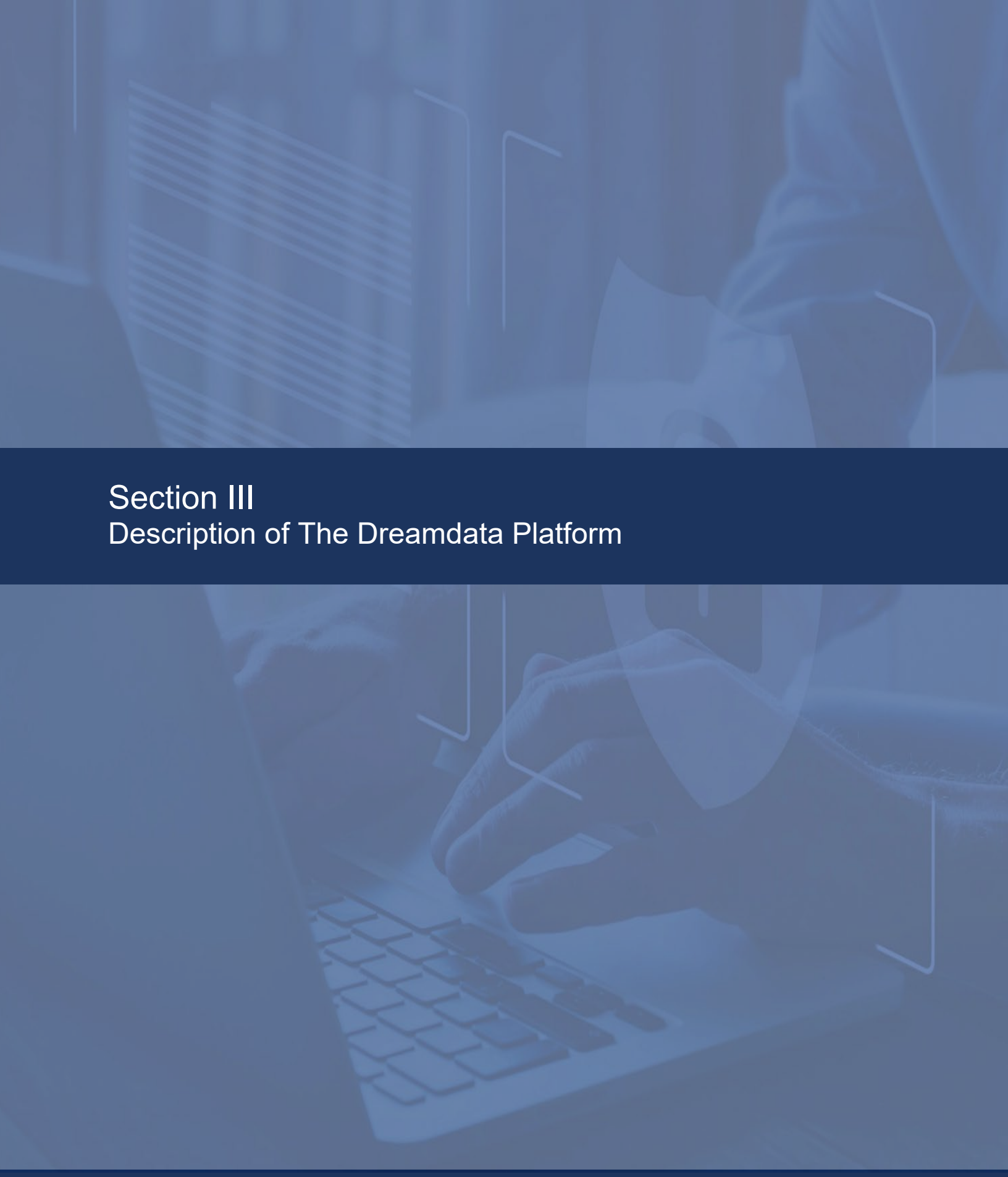
We have performed an evaluation of the effectiveness of the controls within the system throughout the period March 20, 2025 to March 20, 2026, to provide reasonable assurance that Dreamdata.io ApS Dreamdata.io ApS's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria.*

Dreamdata.io ApS Dreamdata.io ApS's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the accompanying system description.

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

We assert that the controls within the system were effective throughout the period March 20, 2025 to March 20, 2026, to provide reasonable assurance that Dreamdata.io ApS Dreamdata.io ApS's service commitments and system requirements were achieved based on the applicable trust services criteria.

Dreamdata.io ApS Management
April 30, 2026



Section III
Description of The Dreamdata Platform

III. Description of The Dreamdata Platform

Company Background

Dreamdata.io ApS was founded in Copenhagen, Denmark, in September 2018, and has employees based in Denmark and the USA.

Dreamdata aims to enable B2B companies to measure their full go-to-market efforts from acquiring leads to closing deals with new customers. Dreamdata gathers data from companies' commercial systems, such as their CRM, marketing automation, paid media, and tracking on their website. Dreamdata then joins and cleans all revenue-related data to present a transparent, actionable analysis of what drives B2B revenue.

Dreamdata was founded by a group of veteran entrepreneurs from Trustpilot and Airtame with deep experience in product management, marketing, go-to-market, data integration, cloud infrastructure, and data analytics. Dreamdata is backed by InReach Ventures, Crowberry Capital, Seedcamp, and angel investors.

Description of Services Overview or Services Provided

The Dreamdata product makes it incredibly easy for go-to-market teams to join data from all systems containing information about the customer journey into one unified customer journey data model containing ad spend, user actions, and business outcomes. This enables actionable analytics such as Revenue attribution and revenue-based performance analytics.

Dreamdata offers a tracking infrastructure for collecting event-level data, connections to products that generate event-level data, and connections to major go-to-market tools to extract event-level data and business outcomes. The setup is self-service, and once systems are connected, Dreamdata builds data models and provides the Dreamdata app automatically.

Users can access the analytics in the Dreamdata app or connect directly with the data models in their data warehouse.

Principal Service Commitments and System Requirements

Dreamdata.io ApS designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Dreamdata.io ApS makes to user entities, the laws and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Dreamdata.io ApS has established for the services. The system services are subject to the Security commitments established internally for its services.

Security commitments to our customers are documented and communicated in our customer agreements (terms and conditions) and, in some cases, in separate SLA agreements, in answers given to security questionnaires, and in reports on our security and data handling provided to customers.

Security Commitments

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

- System features and configuration settings are designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.

- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system.
- Regular vulnerability scans over the system and network, and penetration tests over the production environment.
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Use of data retention and data disposal.
- Uptime availability of production systems.

Components of the System

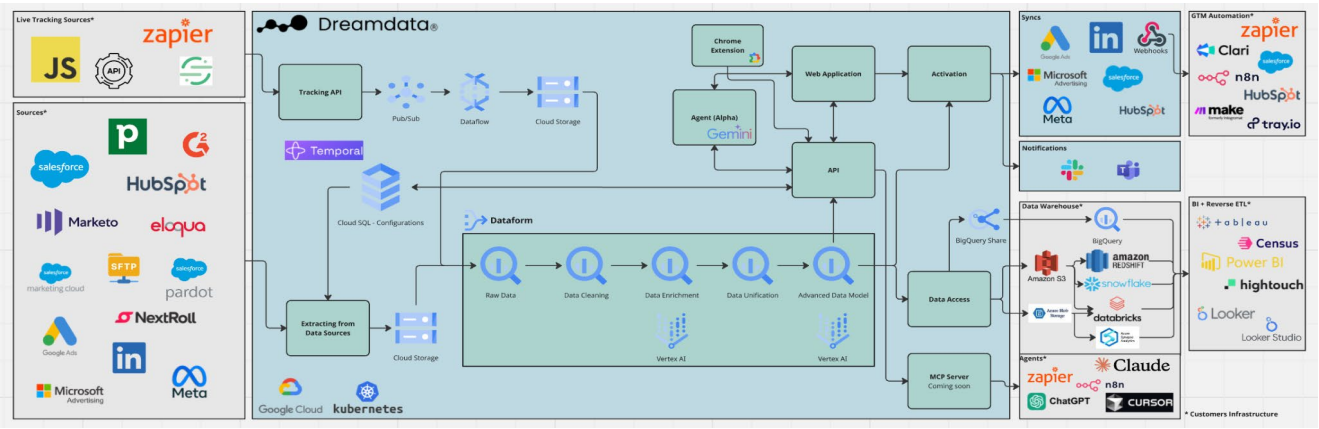
The System description is comprised of the following components:

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

Infrastructure

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

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Google Cloud Server	Hosting	Outsourced hosting provider
Cluvio	Dashboards	Embedded data dashboards



Software

Dreamdata.io ApS is responsible for managing the development and operation of the Dreamdata Platform system, including infrastructure components such as servers, databases, and storage systems. The in-scope Dreamdata.io ApS infrastructure and software components are shown in the table provided below:

Primary Software		
System/Application	**Operating System**	**Purpose**
BigQuery	Linux	Analytical database/data warehouse
PostgreSQL	Linux	Transactional database
Go	Linux	Primary development language for all Infrastructure and ETL systems
Python	Linux	Secondary development language for all Infrastructure and ETL systems
NodeJS	Linux	Primary development language for building APIs
ReactJS	Linux	Primary development language for frontend applications
Temporal	Linux	Data and Process Orchestration System

People

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

Dreamdata.io ApS has a staff of approximately 80, organized in the following functional areas:

- Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.
- Product and Technology Operations: Product managers, designers, and software engineers who design and maintain the Dreamdata product. The team works on data infrastructure, data models, data science, and the Dreamdata web app.
- Admin: Running general operations such as HR and Finance.
- Go To Market: The team responsible for generating demand for the product, capturing that demand through sales, and supporting customers after purchasing the product.

Data

Data, as defined by Dreamdata.io ApS, constitutes the following:

There are 2 major types of data used by the Dreamdata product:

- Customer's Data about its own business: Data owned by Dreamdata's customers that Dreamdata processes on behalf of the customer
- Customer's Data about its customers: Data owned by Dreamdata's customers that Dreamdata processes on behalf of the customer

Customer's Data about its own business contains data about the customers' sales process and includes information about its sales, flow of customers, and flow through their customer acquisition process. The data also contains email addresses and names of the customer's employees (in the form of employees assigned to work on specific accounts). This data is typically extracted from the customer's CRM system. The data is processed and stored in a Dreamdata-owned instance of Google BigQuery.

Customer Data about its customers includes customers' email addresses, names, phone numbers, and behaviors as tracked on the customer's website and in the customer's own systems, such as CRM and marketing automation systems. This data is generated by the customer's own tracking system or the Dreamdata tracking system and extracted from the customer's CRM system and other systems. The data is processed and stored in a Dreamdata-owned instance of Google BigQuery.

Both types of data are processed together in BigQuery into a single data model that the customer can move into their own data warehouse or access through the Dreamdata user interface.

Data is categorized into the following major types of data used by Dreamdata.io ApS:

Category	Description	Examples
Customer data	Information received from customers for processing or storage by the company. Dreamdata.io ApS must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Customer's customers' PII • Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by Dreamdata.io ApS to operate the business. Dreamdata.io ApS must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries

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

All personnel and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Dreamdata.io ApS has policies and procedures in place for proper and secure handling of customer data. These policies and procedures are reviewed at least on an annual basis.

Processes and Procedures

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

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

Physical Security

Dreamdata.io ApS's production servers are maintained by Google Cloud Platform. The physical and environmental security protections are the responsibility of Google Cloud Platform. Dreamdata.io ApS reviews the attestation reports and performs a risk analysis of Google Cloud Platform on at least an annual basis.

Logical Access

Dreamdata.io ApS provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes.

Access to these systems is split into admin roles, user roles, no access roles, and Engineering/Data Scientist. User access and roles are reviewed on an annual basis to ensure least privilege access.

InfoSec/IT is responsible for provisioning access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Dreamdata.io ApS's policies and completing security training. These steps must be completed within 14 days of hire.

When an employee is terminated, InfoSec/IT is responsible for deprovisioning access to all in-scope systems within 3 days of that employee's termination.

Computer Operations - Backups

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

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

Computer Operations - Availability

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

Dreamdata.io ApS internally monitors all applications, including the web UI, databases, and cloud storage, to ensure that service delivery matches SLA requirements.

Dreamdata.io ApS utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open source dependencies and maintains an internal SLA for responding to those issues.

Change Management

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

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system. Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

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

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

Dreamdata employs vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues. Dreamdata conducts external penetration tests on an annual basis in combination with it's full time bug bounty program.

Boundaries of The System

The boundaries of the Dreamdata Platform 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 Dreamdata Platform.

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

The Applicable Trust Services Criteria and The Related Controls

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

Control Environment

Integrity and Ethical Values

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

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

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

Commitment to Competence

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

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

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

Management's Philosophy and Operating Style

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

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

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

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

Organizational Structure and Assignment of Authority and Responsibility

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

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

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

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

Human Resource Policies and Practices

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

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

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

Risk Assessment Process

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

Integration with Risk Assessment

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

Information and Communication Systems

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

Dreamdata.io ApS uses several information and communication channels internally to share information with management, employees, contractors, and customers. Dreamdata.io ApS uses chat systems and email as the primary internal and external communications channels.

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

Monitoring Controls

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

On-Going Monitoring

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

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

Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high

rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System

No significant changes have occurred to the services provided to user entities during the review period or since the organization's last review.

Incidents

No significant incidents have occurred in the services provided to user entities during the review period or since the organization's last review.

Criteria Not Applicable to the System

No significant incidents have occurred in the services provided to user entities during the review period or since the organization's last review.

Subservice Organizations

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

Subservice Description of Services

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

Complementary Subservice Organization Controls

Dreamdata.io ApS's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Dreamdata.io ApS's services to be solely achieved by Dreamdata.io ApS's control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Dreamdata.io ApS. The following subservice organization controls have been implemented by Google Cloud Platform and included in this report to provide additional assurance that the trust services criteria are met.

Subservice Organization – Google Cloud Platform (GCP)		
Category	**Criteria**	**Control**
Security	CC 6.4	Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge access readers, biometric identification mechanisms, and/or physical locks.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high-security areas in data centers are reviewed on a defined basis, and inappropriate access is removed in a timely manner.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.

		Security measures utilized in data centers are assessed annually, and the results are reviewed by executive management.
		Data centers are continuously staffed and monitored by security personnel using real-time video surveillance and/or alerts generated by security systems.

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

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

Complementary User Entity Controls

Dreamdata.io ApS's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Dreamdata.io ApS's services to be solely achieved by Dreamdata.io ApS's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Dreamdata.io ApS.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

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