



Dataddo, a.s.
Prague, Czech Republic

SYSTEM AND ORGANIZATION CONTROLS (SOC) 3
REPORT

REPORT ON CONTROLS AT SERVICE ORGANIZATION
RELEVANT TO DESCRIPTION OF DATADDO, A.S. SYSTEM
AND ON THE SUITABILITY OF THE DESIGN AND
OPERATING EFFECTIVENESS OF CONTROLS TO MEET
THE CRITERIA FOR THE SECURITY, AVAILABILITY,
CONFIDENTIALITY, AND PROCESSING INTEGRITY.

THROUGHOUT THE PERIOD
2023-03-01 THROUGH 2024-02-29





TABLE OF CONTENTS

TABLE OF CONTENTS	1
I. INDEPENDENT SERVICE AUDITOR'S REPORT	4
II. MANAGEMENT OF DATADDO SERVICE ORGANIZATION'S ASSERTION.....	7
III. ATTACHMENT A	9
DESCRIPTION OF THE BOUNDARIES OF THE DATADDO SYSTEM	9
DATADDO PROFILE	9
Key features of Dataddo	9
Basic components	9
ORGANIZATIONAL STRUCTURE	11
POLICIES AND PROCEDURES	12
CODE OF CONDUCT AND ETHICS	13
DATA PRIVACY AND PROTECTION	13
COMMUNICATION	14
RISK ASSESSMENT PROCESS.....	14
PHYSICAL SECURITY	15
ACCESS CONTROL	15
INFRASTRUCTURE	16
ENDPOINT PROTECTION	16
CHANGE MANAGEMENT	17
DISASTER RECOVERY	18
VULNERABILITY MANAGEMENT.....	19
Servers	19
End stations	19
IV. ATTACHMENT B	21
DESCRIPTION OF A DATADDO SERVICE ORGANIZATION'S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS	21
SECURITY	22
AVAILABILITY	22
CONFIDENTIALITY	22
PROCESSING INTEGRITY.....	23



EXECUTIVE SUMMARY

Scope	DATADD0, a.s.
Period of Examination	March 1, 2023 to February 29, 2024
Applicable Trust Principle(s)	Security, Availability, Processing Integrity, and Confidentiality
Location (s)	Prague, Czech Republic
Subservice Providers	MongoDB, Inc. Amazon AWS
Opinion Result	Unqualified

I. Independent Service Auditor's Report

I. INDEPENDENT SERVICE AUDITOR'S REPORT

To: Board of Directors of Dataddo, a.s.

Scope

We have examined Dataddo, a.s. Service Organization's ("Dataddo" or the "service organization") a companying assertion titled "Dataddo Service Organization's System Assertion" (assertion) that the controls within Dataddo's transportation management system (system) were effective throughout the period March 1, 2023 to February 29, 2024 to provide reasonable assurance that Dataddo's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 (update 2022) *Trust Services Criteria for Security, Availability, Processing Integrity and Confidentiality in AICPA Trust Services Criteria*.

Service Organization's Responsibilities

Dataddo 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 Dataddo's service commitments and system requirements were achieved. Dataddo has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Dataddo is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period March 1, 2023 to February 29, 2024, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Dataddo uses Microsoft Azure (Azure) and Amazon AWS, a subservice organization, to provide infrastructure as a service. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Dataddo, to achieve Dataddo's service commitments and system requirements based on the applicable trust services criteria. The description presents Dataddo's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Dataddo's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice

organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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 controls were not effective to achieve Dataddo's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Dataddo's service commitments and system requirements based on the applicable trust services criteria

Inherent Limitations

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 Dataddo's transportation management system were effective throughout the period March 1, 2023 to February 29, 2024, for Dataddo to provide reasonable assurance that Dataddo's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



BDO Consulting s.r.o.

07.03.2024

II. Management of Dataddo Service Organization's Assertion

II. MANAGEMENT OF DATADDO SERVICE ORGANIZATION'S ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within Dataddo Service Organization's (Dataddo's) transportation management system (system) throughout all of the period: March 1, 2023 to February 29, 2024, to provide reasonable assurance that Dataddo's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 (update 2022) Trust Services Criteria for Security, Availability, Processing Integrity and Confidentiality in AICPA Trust Services Criteria. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout all of the period: March 1, 2023 to February 29, 2024, to provide reasonable assurance that Dataddo's service commitments and system requirements were achieved based on the applicable trust services criteria. Dataddo's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

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

We assert that the controls stated in the description operated effectively throughout all of the period: March 1, 2023 to February 29, 2024, to provide reasonable assurance that Dataddo's service commitments and system requirements were achieved based on the applicable trust services criteria.

III. Attachment A
Description of the boundaries of the
Dataddo system

III. ATTACHMENT A

DESCRIPTION OF THE BOUNDARIES OF THE DATADDO SYSTEM

DATADDO PROFILE

Dataddo was founded in Prague in 2018 and is now headquartered in the heart of Silicon Valley. Dataddo currently serves more than 3000 organizations and individuals from 100+ countries, including some of the world's most recognizable brands. We're proud to be named a 2019 Cool Vendor in Data Management by Gartner.

Despite incredibly diverse offerings in the field of data analytics, we saw the need for increased flexibility. That's why we created Dataddo - a single no-coding platform for data integration, automation, and transformation. With the vision to give people full control of and access to their own data, we designed Dataddo to work with any online data service, including the data architecture they already have.

Key features of Dataddo

- Out-of-the-box, no-code connectors to many different cloud-based services such as Salesforce, Hubspot, Google Analytics, and more.
- Automatic data synchronization between data sources and storage solutions.
- Integrated persistence layer for lightweight cases not requiring a data warehouse.
- Ability to quickly provision a custom connector.
- Centralized pipeline management and proactive monitoring.
- Data quality checks
 - Avoiding duplicities
 - Anomalies detection
 - Time series gap detection
- No-code data blending and transformations
- Direct connections with popular BI apps (e.g. PowerBI, Tableau, Google Data Studio) without the need for a data warehouse.

Basic components

Sources

When 3rd party services are connected to Dataddo and a dataset definition is set, it is referred to as a source. Most marketing data sources like Facebook Ads, Google Analytics, and others only require one source for each account or page. Depending on your data requirements, other services may require multiple connections in order to provide all of the desired data pertaining to a specific account.

Synchronization

Advanced operations for working with sources within Dataddo. Easily configure automatic data extraction from your sources and operate all sources from one place.

Third-party account authorization

When you want to connect third-party accounts like Salesforce, Hubspot, Google BigQuery, or any other, it is necessary to authorize it before you connect with Dataddo. Authorizing takes just a few seconds and can be done from your profile settings within Dataddo.

External storages

Dataddo can deliver your data to any location and easily connect various data storage technologies such as Google Big Query or AWS Redshift, SQL-based databases, even SFTP servers. You can easily manage all the connections from our interface.

Data flow

The data flow is a central part of the Dataddo system which orchestrates all of the integrations. You can easily configure the data flow to sync data from source to destination at particular timings and intervals.

ORGANIZATIONAL STRUCTURE

1. Dataddo, a.s. is a joint-stock company and its legal status, subject of business, shareholders' competencies and the manner and forms of exercising these competencies are determined by the company's articles of association.
2. The registered office of Dataddo, a.s. is Piletická 486, 503 41 Hradec Králové - Věkoše
3. Legal status, subject of business and other requisites of business activity of the company Dataddo, a.s. The following documents in particular document:
 - Articles of Association of Dataddo, a.s.
 - Certificate of Incorporation
 - Tax registration certificate
 - Extract from the trade register
 - Legal documents associated with the establishment of subsidiaries

Company parts:

A. In accordance with the company's Articles of Association, the Civil Code and the Commercial Corporations Act, the following bodies of Dataddo, a.s. are established:

- General Meeting,
- Board of Directors,
- Supervisory Board.

B. The General Meeting is the highest body of the company. Through it, shareholders exercise their rights under the Articles of Association and generally binding legal regulations. The powers of the general meeting of the company are exercised by a single shareholder.

C. The Board of Directors is the statutory body of the company, which has the management of the company and all the powers that the articles of association or the law do not entrust to another body. The Board of Directors has 1 member. The members of the Board of Directors are elected and removed by the General Meeting. The term of office of individual members of the Board of Directors is 10 years.

D. The Supervisory Board is the company's supervisory body and supervises the exercise of the powers of the Board of Directors. The Supervisory Board has 3 members, who are elected and removed by the General Meeting. The term of office of a member of the Supervisory Board is 10 years.

Structure:

- CEO
 - Security Manager
 - Head of product
 - CTO
 - Development department
 - Monitoring department

- IT Support
- COO
 - Finance department
 - Legal
 - HR
 - BOZP Manager
 - Risk Manager
 - QMS Manager
- CCO
 - Sales department
 - Marketing department
 - Solutions department
 - Customer success department

POLICIES AND PROCEDURES

Dataddo a.s. is aligned organizationally around the web service www.Dataddo.com. Dataddo a.s. leverages some aspects of Amazon's overall control environment in the delivery of these web services. The collective control environment encompasses management and employee efforts to establish and maintain an environment that supports the effectiveness of specific controls. Dataddo maintains internal informational services describing the Dataddo service and environment, its boundaries, user responsibilities and services.

The control environment at Dataddo a.s. begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's core values and tone at the top. The Company's Code of Business Conduct and Ethics, which sets guiding principles, is made available to every employee.

Dataddo a.s. is committed to having the highest qualified members as a part of its Board of Directors.

Dataddo is committed to protecting its customers' data and maintaining compliance with applicable regulatory requirements. This is demonstrated by the consolidated annual risk assessment, that includes regulatory and compliance requirements and objectives to enable the identification and assessment of risks relating to those objectives.

Dataddo's policies and procedures outline the required guidance for operation and information security that supports the AWS environment, acceptable use of mobile devices, and access to data content and network devices.

All Dataddo a.s. employees are required to review all applicable policies and procedures, as updated from time to time. Evidence of compliance with the training on Dataddo policies is executed and retained by the employee resource team (HR).

Dataddo a.s. has set up an ethics hotline for the employees (called "Inbox") or third-party contractors (webform) to report any misconduct or violation of Dataddo policies, practices, rules, requirements or procedures.

Any material violation of the Company Code of Business Conduct and Ethics or any other similar policies are appropriately handled accordingly which may include disciplinary action or termination of employment. Violations by vendors or third-party contractors are reported to their employers for disciplinary action, removal of assignment with Dataddo, or termination.

Dataddo performs a formal evaluation of the appropriate resourcing and staffing, to align employee qualifications with the entity's business objectives to support the achievement of the entity's business objectives. Appropriate feedback is given to the employee on strengths and growth areas during the annual performance review process. Employee strength and growth evaluations are shared by the employee's manager with the employee.

The Dataddo Security team (CTO, COO, Security manager) has established an information security framework and regularly reviews and updates the security policies, provides security training, which includes data classification, to employees, and performs application security reviews. These reviews assess the availability, confidentiality, and integrity of data, as well as conformance to the security policies.

CODE OF CONDUCT AND ETHICS

The Code of Ethics is a basic document describing the principles of ethical behavior of Dataddo a.s. (hereinafter referred to as the "employer"). Its goal is to set a common understanding of their manifestations in everyday work practice for shared values. The Code of Ethics is a binding document for all employees and members of the employer's bodies (hereinafter for the purposes of this Code of Ethics collectively as "employees"). One of the basic principles on which the Code is based is based on the fact that employees are aware that their actions may expose employers and themselves to criminal, administrative or civil penalties. Therefore, they act in such a way that there is no criminal offense or other violation of legal and internal regulations. The employer does not tolerate any breach of the Code of Ethics and may also consider it a serious breach of duty. The Code of Ethics is an expression of our commitment to ethical conduct to partners, users and colleagues.

DATA PRIVACY AND PROTECTION

Dataddo is committed to protecting the security and confidentiality of the data of its customers and business partners ("customer data"). Confidentiality clauses ensure this in agreements with business partners and employees. Security is further enhanced by restricting access to sensitive data. Access to customer data is granted to employees on a need-to-know basis, and data is fully encrypted at rest and in transit.

Customers have complete control over their content and are ultimately responsible for how data is managed after being exported.

Dataddo has developed and implemented plans and incident response guidelines for responding to data breaches in accordance with customer agreements.

COMMUNICATION

The board and management meet on regular basis. For internal IT the interval is set once a week, for the product meetings are done bi-weekly. These meeting are conducted offline or online. The company uses separate communication lines. For internal communication is set Slack as primary channel. The whistleblowing line is also implemented.

RISK ASSESSMENT PROCESS

Dataddo a.s. maintains a formal risk management program to continually discover, research, evaluate, plan, resolve, and optimize information security risks that impact Dataddo a.s. business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, mitigation.

A formal risk matrix is updated at least annually. Dataddo Risk manager and reports risks to Dataddo Management on an annual basis. Dataddo Management acknowledges risk treatment decisions and formally approves risk acceptance. The risk management program consists of the following phases:

- 1. Discover** - During the discovery phase, the risk management team characterizes and documents technical and business risks to the organization and operations. A basic understanding of the risk and its relationship to the customer and Dataddo is also established.
- 2. Research** - During the research phase, the risk management team gathers information and conducts interviews to understand the risk in greater detail. Research includes factors that may impact the successful delivery of Dataddo product and services, protection of customer and company assets, the business and regulatory environment, and other potential threats to the security of customer and company resources.
- 3. Evaluate** - During the evaluate phase, the risk management team assesses the potential severity and scope of the risk. Threats, vulnerabilities, and assets are identified and the risk is mapped to and evaluated against Dataddo security controls. The threats, vulnerabilities, assets, previous research data and effectiveness of AWS controls are analyzed to rate the inherent and residual severity of the risk.
- 4. Plan** - During the plan phase, a risk treatment approach is selected and high-level milestones for risk treatment are defined. The key stakeholders and partners to support the risk treatment plan are identified.
- 5. Resolve** - During the resolve phase, the risk management team works with relevant partners to monitor implementation of the treatment plan specific to the risk. The risk management team also assists the partner team as needed and provides risk guidance to facilitate successful risk treatment. The risk management team updates its evaluation of the risk based on the outcomes of treatment.
- 6. Optimize** - During the optimize phase, the risk management team reviews and monitors how well the risks are treated and plan for any further actions as appropriate, manage the success of individual risk treatment plans, and adjust the program as needed.

On an annual basis, the risk management team compiles a risk report which summarizes all risks and highlights what the business needs to know about risk.

PHYSICAL SECURITY

Dataddo services and service components are without the possibility of physical contact or on-site service for anyone from Dataddo or outside the company.

The access that employees can only receive is access to the company's headquarters in Prague. This access is automatically revoked when an employee's record is terminated in Dataddo's HR system. Cardholder access to Dataddo is reviewed quarterly. Cardholders marked for removal have their access revoked as part of the review.

Physical access is controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. All the servers providing the production services are located in the AWS cloud and Dataddo itself has no own server room. Dataddo uses their protected end-stations to connect to the cloud environments.

ACCESS CONTROL

The access control is managed on multiple levels. Each employee has granted his own user account and roles in google administration according to their real roles and positions in the company. Dataddo follows the least privilege principles and is granting the roles and access only to people who necessarily need it. According to the position, the user is granted access to also other tools and services. When possible we use the Google SSO mechanism to use the already existing Google account. In case of the user contract termination we remove the Google account which prevents accessing all services using SSO automatically too.

Selected users are granted to access the VPN. Only roles which the company requires to access internal services are granted the access and their list is regularly reviewed. Even the smaller subgroup of such users can access the infrastructure itself (test environment). Typically developers can access the dev and test environment components. The users with the most wide privileges are the infra administrators and the most senior engineers who can even access the production environment.

Access Removal

Access is revoked when an employee's record is terminated in Dataddo's HR system. The revoke access right process is established and all user accounts are suspended or deleted immediately.

Password Policy

Access and administration of logical security for Dataddo relies on user IDs and passwords. Based on the concrete username or assigned role the user is granted permissions to access various levels of the Dataddo infrastructure. Dataddo Security has established a password policy with required configurations and expiration intervals. Whenever possible users are forced to use MFA. Dataddo uses Google SSO to all major services where this auth mechanism is available.

Remote Access

Dataddo requires VPN access over an approved cryptographic channel for authentication to the internal AWS Dataddo network from remote locations using Wireguard VPN.

INFRASTRUCTURE

Dataddo has all of its infrastructure in the cloud. It mainly uses AWS as a cloud provider, but some tools and helping applications are also run in Azure and in Google Cloud.

The whole production environment runs in the AWS environment. The default location for compute and storage is eu-west-1, but for storing the customer data Dataddo offers also other geographical locations to store the data in.

The Dataddo infrastructure is split into multiple environments (also separate AWS accounts). There are the environments for production, staging/testing environment, development, shared environment for app builds/images. The whole production traffic and processing is done within the production AWS account.

Whenever possible Dataddo uses managed services by the cloud provider. This is applicable to the security (AWS Cognito - for storing users credentials, AWS KMS - for any data encryption) and also for the data storages (AWS RDS with postgres, AWS ElastiCache redis, MongoDB Cloud). Using managed services with SLA with the cloud vendor gives Dataddo guarantees in terms of high availability of the services. The Dataddo's internal availability and disaster recovery policy benefit from using such services with high guarantees.

As mentioned before, Dataddo also has a testing environment where the same components are spinned up the same way as they are in the production environment. All the changes and modifications are at first tested in the testing environment prior to their release to the production environment.

ENDPOINT PROTECTION

Dataddo employees use Mac or Linux stations for work. All the servers are linux. Only the skilled senior engineers are allowed to use the Linux endpoint stations. All Mac endpoints are protected by the ESET Endpoint Security, which provides comprehensive protection for stations, the ability to define firewalls and corporate policies. By using this tool we have a nice overview of the statuses of the stations including their system versions, installed apps and also monitor vulnerabilities these stations face.

Another part of this endpoint security system is the management server. Console management with status reporting of individual computers, where it is possible to manage and control individual endpoints (computers).

Each computer is required to have all security patches implemented within 48 hours of the detection of a serious problem, an encrypted disk and firewall enabled at the system level, and all system components and drivers updated according to its authors and recommendations.

We also use Hexnode MDM for device management of the end stations. In Hexnode MDM we have policies applied to all Dataddo endpoint devices (password requirements policy, data encryption policy, firewall policy). We can also deactivate or prune devices remotely in case of theft or loss of the device. Having the Dataddo device does not automatically grant access to any systems. To access internal systems and tools the valid authorization with the company Google account is a must (we can remotely log out users from the services in case of need). Other services (servers, databases, etc.) required the VPN

connection which is available only to a limited group of Dataddo employees. The access to the VPN can be rejected remotely too without access to the end station.

CHANGE MANAGEMENT

Dataddo applies a systematic approach to managing change so that all code and infrastructure or services changes are reviewed, tested, approved, and well communicated.

The change management processes are based on the Dataddo's change management guidelines and tailored to the specific services. These processes are documented and communicated to the necessary personnel by service team management.

The goal of Dataddo's change management process is to prevent unintended service disruptions and maintain the integrity of service to the customer alongside with keeping the services secure.

Change details are documented in Dataddo's change management policy..

Prior the change gets to production environments, the steps to follow are:

- **Develop:** during the development the dev environment that is segregated from the production environment is used. Customer content is not used in the development environment. Dataddo uses source code version control system Git for all application and infrastructure changes.
- **Test:** Dataddo uses automated Continuous Integration (CI) pipelines to test the code changes in an automated way. We check the code style, run automated tests, check for the outdated libraries, scan for vulnerabilities in packages etc.
- **Approve:** Every change is usually subjected to something called "Merge Request". Merge request encapsulates the new code changes and the intended change waits in the VCS until it is approved by a senior engineer. This follows the principle of at least 4-eyes checking the change (author + reviewer). The reviewer checks the intended changes for possible malfunctions/bug or for security threats. When the change is approved by the reviewer the code change is merged into the main source code version.
- **Staging:** After the code change is merged to the main source code, the application is built into the working docker image with specific version (for possible later easy version rollback). Then this version is automatically deployed to the staging/testing environment, which is nearly identical to the production one. Here another set of automated tests are performed in order to assure us that intended change works as expected and other parts of the system are not affected in any negative way. Also the manual testing can be performed at this stage by the developers, product or QA team.
- **Production:** When the code change is accepted in the testing environment, the senior engineers create the "Merge request" to the production environment. Another set of automated checks can be performed at this stage again. Our Continuous Delivery (CD) pipeline automatically deployed the change to the production server.
- **Deployment strategies:** According to the service criticality or possible risk of the code change, the different deployment strategies may be used. In case of minor changes when engineers are pretty sure about the change, the change can be deployed to all the replicas of that service. In some cases we tend to use more conservative ways of deploying new changes like canary releases or blue/green deployments. For some sensitive issues or for A/B testing of new code we use the

feature flags, by which we can enable/disable selected code changes live from the external tool.

- **Rollbacks:** Every Dataddo production service has the option of rollbacks to previous versions. When we identify some code change is causing troubles or malfunctioning of our services we have the option to return to the previous version which was safe. It always depends on the senior engineers or team leader's decision if the rollback should be done or if it is better to put the fix code change into the code base.
- **Monitoring:** The deployment of the code change to the production is not the last part. We also monitor the behavior of our services using our monitoring tools which tell us the error rates, the resources consumption (cpu, memory, fds, ...) on various levels of our infrastructure. The team leaders of the development teams are responsible for monitoring such metrics and plan code changes and tickets also according to their investigations.

When possible, changes are being deployed continuously and the pressure from Dataddo management is to deploy frequently and the small pieces of change instead of planned big release (e.g. once a week or month). Emergency changes to production systems that require deviations from standard change management procedures are associated with an incident and are logged and approved as appropriate.

Dataddo performs the validations of roles involved in the change management process regularly to assure only skilled engineers may deploy to the production systems etc. These validation checks are part of the regular user management process checks. Dataddo team leaders and management also continuously reviews and tracks deployment violations for services based on reports in the monitoring tool.

DISASTER RECOVERY

The company has developed procedures and instructions for the data recovery process for each service, the data recovery process is based on the assumptions and products of cloud providers and their features described below, this process takes into account and uses them.

All data stored in AWS (AWS RDS postgres) and Mongo Cloud (MongoDB) are regularly backed up with the interval and retention settings in compliance with Dataddo requirements and needs. If corruption is detected, Dataddo can easily return to the previous snapshot of the data. All the application services developed by Dataddo are stateless, which means they use previously mentioned technologies to store the data for them. This leads to the fact that the failures of the applications have minimal impact on the possibility of losing some data etc.

Dataddo also does extra backups of all important data using a custom tool which does the full backups of Dataddo databases every hour. This means that at any point, Dataddo has at most 1-hour old data which can be recovered. This backup process is automatically monitored and the status of such backups is internally tested on a daily basis by restoring the data every day.

The whole production/testing/shared and other Dataddo accounts infrastructure is managed as infrastructure-as-a-code (declarative) with all the source code in the version control. Dataddo uses the terraform tool to automate the spinning up the production or

doing any updates there. Thanks to this setup, Dataddo can easily see if the infrastructure is not aligned with the definition in the source code and possibly to create the whole infrastructure components in the matter of hours.

VULNERABILITY MANAGEMENT

When speaking about vulnerabilities we may divide this field into two segments:

- servers
- end stations

Servers

The operational servers are taken care of by the automated monitoring. The monitoring is performed internally by Dataddo engineers, but also externally by the 3rd party vendor who is responsible mainly for monitoring of networking and hardware/cloud/infrastructure (servers, kubernetes, etc.) level, whereas Dataddo internally focuses primarily on monitoring the application layer. Both levels may overlap in some technologies. The infrastructure and tools being used there are patched and updated on a regular basis according to the plan agreed with our 3rd party vendor. The production environment is usually updated twice a year when usually the EC2 AMI images are updated, Kubernetes and other related tools versions are updated, the new terraform modules are being used etc. The application layer updates are performed on a daily basis and all the development teams use the latest version of libraries and vendor tools if possible. Dataddo also regularly orders the penetration testing of their infrastructure from the independent 3rd party vendor which results are discussed during regular security meetings and findings are evaluated and possibly materialized in tasks for development.

End stations

End stations are used as thin clients when accessing the cloud environment, therefore no customer data are being kept there. There are user management policies in places following the least privileges principle and the users are granted the access they really need in order to perform their job duties. All the Dataddo computer end stations are mac machines which have the ESET antivirus installed and maintained via remote ESET console. All such machines are also registered in Hexnode MDM which is used to enforce some security policies and may be used to wipe or block the stolen device remotely etc.

IV. Attachment B
Description of a Dataddo service
organization's principal service
commitments and system requirements

IV. ATTACHMENT B

DESCRIPTION OF A DATADDO SERVICE ORGANIZATION'S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Service Commitments

Commitments are declarations made by management to customers regarding the performance of the Dataddo Commitments to customers are communicated via Service Level Agreements, and/or Data Processing Agreements. Data Processing Agreements define the security and privacy obligations which the processors must meet to satisfy the organization's obligations regarding the processing and security of customer data.

System Requirements

System requirements are specified in the Dataddo's policies and procedures, which are available to all employees.

Dataddo makes service commitments to its customers and has established system requirements as part of Azure and AWS service. Some of these commitments are principal to the performance of the service and relate to applicable trust services criteria. Dataddo 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 Dataddo service commitments and system requirements are achieved.

Dataddo is subject to relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Dataddo operates.

Security, Availability, Confidentiality and Processing Integrity commitments to customers are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided on the Dataddo website. Security, Availability, Confidentiality and Processing Integrity commitments are standardized and include, but are not limited to, the following:

- Security and confidentiality principles inherent to the fundamental design of the Dataddo System are designed to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.
- Security and confidentiality principles inherent to the fundamental design of the Dataddo System are designed to safeguard data from within and outside of the boundaries of environments which store a customer's content to meet the service commitments.
- Availability principles inherent to the fundamental design of the Dataddo System are designed to replicate critical system components across multiple Availability Zones and authoritative backups are maintained and monitored to ensure successful replication to meet the service commitments.

- Processing integrity principles inherent to the fundamental design of the Dataddo System are designed to protect the security and confidentiality of Dataddo customer data in transit to meet the service commitments.

Dataddo establishes operational requirements that support the achievement of security, availability, confidentiality and processing integrity commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Dataddo system policies and procedures, system design documentation, 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 the system is 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 various Dataddo services and offerings. Dataddo Technologies' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality and processing integrity.

SECURITY

Dataddo security measures are designed to protect information and assets from unauthorized access, loss, damage or misuse. Key measures include the management of logical and physical access and the application of established and implemented policies and procedures. The organisation actively uses data encryption and resources and tools to protect the network and regularly performs systems checks to ensure security and identify potential security risks. Risk management is regularly performed in the company. Dataddo monitors and detects threats and incidents, providing the ability to respond quickly to cyber-attacks and other security incidents.

AVAILABILITY

The organization uses cloud services to allow for scalable infrastructure and monitors its systems based on utilization and critical production resources for health and capacity issues. Infrastructure monitoring tools are implemented to monitor IT infrastructure and maintain security, availability and performance. Alerts are generated when specific conditions are met.

On premise servers are used in DC for the defined scope of services. Monitoring solution for the services is implemented and operating. Dataddo has established a BCP to maintain or restore operations and ensure availability of information at required level; detection measures are in place, including monitoring of the events.

CONFIDENTIALITY

Dataddo communicates confidentiality commitments and responsibilities through standard Service Agreements to vendors and other third parties.

Policies and procedures regarding confidentiality are implemented. Data retention schedule is part of Data retention policy. Classification of information assets is reviewed periodically by their owners.

If customer distributes information that is classified as confidential, customer is informed about Dataddo's standardized solution and further confidential information is shared

through secured repository. Other specific aspects such as data sanitation; secure data disposals are considered accordingly.

PROCESSING INTEGRITY

Policies and procedures regarding processing integrity are implemented. A data retention plan is part of the data retention policy. The classification of information assets is regularly reviewed by their owners.

Dataddo maintains the integrity of processing systems through stringent data accuracy and completeness measures. Dataddo change management procedures ensure that all changes to the system are thoroughly tested and implemented without compromising data integrity. Validation checks and reconciliation procedures are systematically carried out to uphold the accuracy and completeness of processed data. Dedicated Dataddo team also monitors the discrepancies in the customer's data flows and are ready to react accordingly to any unusual situation.