Oktober 2025

Adeo Datacenter ApS

CVR 37 59 31 84

ISAE 3402 ASSURANCE REPORT

Independent Auditor's ISAE 3402 assurance report for the period from 1 January 2024 to 31 December 2024 on the description of Adeo Datacenter's services and the related controls and their design and operating effectiveness

Indhold

1. Managements' Statement

The accompanying description has been prepared for Adeo Datacenter's customers and their auditors who have a sufficient understanding to consider the service, along with other information, including information about controls operated by the customers themselves, when assessing the risk of material misstatement of customers' financial statements.

Adeo Datacenter confirms that:

(A) The accompanying description in section 2 fairly presents Adeo Datacenter services related to customer transactions processed throughout the period from 1 January 2024 to 31 December 2024. The criteria used in making this statement were that the accompanying description:

(i) Presents how the system was designed and implemented, including:

- The types of services provided, when relevant
- The procedures, within both information technology and manual systems, by which the IT general controls were managed.
- Relevant control objectives and controls designed to achieve those objectives
- Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone.
- How the system dealt with significant events and conditions other than transactions
- Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to the IT general controls

(ii) Includes relevant details og changes to the controls to the service providers services during the period from 1. January 2024 to 31 December 2024

(iii) Does not omit or distort information relevant to the scope of the controls described relating to services considering that the description is prepared to meet the general needs of a wide range of customers and their auditors and therefore cannot include every aspect of services that the individual customer may consider of importance to their special environment.

(B) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 January 2024 to 31 December 2024. The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified;

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risk did not prevent the stated control objectives from being achieved; and

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 January 2024 to 31 December 2024.

Albertslund, 31. oktober 2025

Adeo Datacenter ApS

Mikkel Emmerik
Adm. Direktør

2. Adeo Datacenter ApS's description of services

Introduction

This description is intended to provide information to Adeo Datacenter's customers and auditors on the requirements of ISAE 3402-II, an international standard for service providers' control assurance. This also includes a description of controls used in Adeo Datacenter's operations from 1 January 2024 to 31 December 2024.

Description of Adeo Datacenter ApS

Adeo Datacenter is a Danish-owned data center established in 2016. It provides data center services within its own facilities located in Albertslund. The employees at Adeo Datacenter bring over 50 years of experience in hosting and data center management, catering to both small and large companies. Solutions are tailored based on customer needs and preferences, whether customers choose to use their own equipment or rent servers and hardware from Adeo Datacenter.

Adeo Datacenter ensures optimal operational stability and security for the entire infrastructure, both in the short and long term. We focus on flexible, easily scalable solutions that benefit customers, the business, and employees, allowing them to concentrate on their core operations.

We are exclusively focused on data center operations for businesses and organizations. Our customer references include independent software vendors (ISVs) and partners, such as companies providing managed IT services.

Our approach is customer-centered, crafting customized solutions from various products with different features, ranging from virtual machines to physical rack cabinets. Adeo Datacenter is classified as a professional data center, offering optimal protection for servers and data. This includes electronic access control, video surveillance, temperature alarms, smoke/fire sensors, climate control, UPS, and generator systems.

The data center is organized into five separate data halls and separate rows with a switch-centric, redundant network infrastructure, allowing for quick and flexible expansion of servers, CPUs, and storage capacity to precisely match customer needs.

At Adeo Datacenter, we are committed to IT security and to complying with the EU's new General Data Protection Regulation (GDPR), effective as of May 2018. As a Danish-owned data center based in Denmark, we take a significant step toward meeting the requirements of this regulation, ensuring that customers know where their data resides—unlike virtual services and competitors with interconnected data centers across multiple countries.

Scope of thes Description

Adeo Datacenter is a provider of data center services, with core activities focused on data center operations. Infrastructure monitoring is managed by Adeo Datacenter, while customers are responsible for monitoring and supporting their own or rented equipment located within the data center.

Adeo Datacenter is responsible for establishing and adhering to appropriate procedures and controls to detect and prevent errors. Compliance with these controls is essential to operations and forms the foundation for an ISAE 3402-II certification.

IT Security Strategy

Adeo Datacenter's strategic focus for IT security is to ensure that the business has built-in mechanisms to prevent unacceptable risks to both the company and its customers.

Our security policy is highly prioritized by management, which is reflected in our daily procedures and business practices.

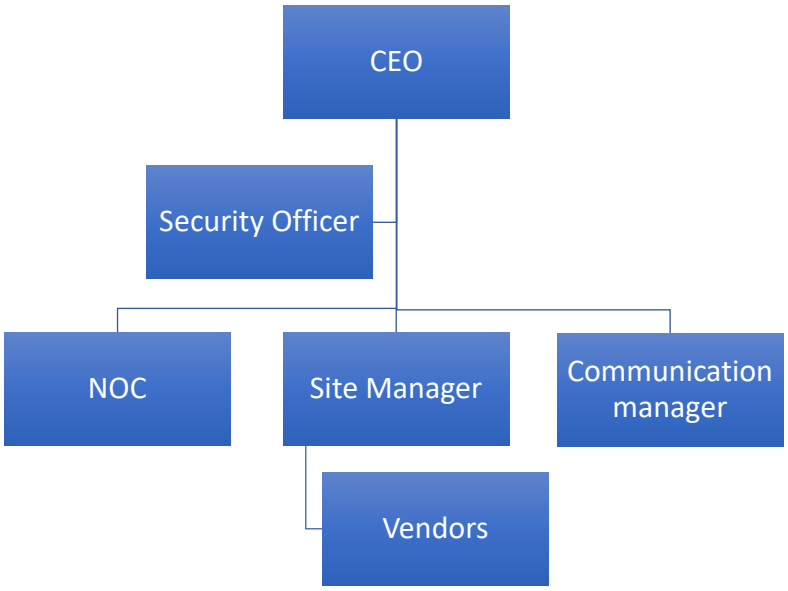
Adeo Datacenter's security policy outlines security measures in the following areas:

- Information Security Policies
- Organization of Information Security
- Employee Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operational Security
- Communication Security
- Acquisition, Development, and Maintenance of Systems
- Supplier Relationships
- Information security incident management
- Information Security Aspects in Emergency, Contingency, and Recovery Management
- Compliance

All procedures are continuously reviewed and revised to optimize and automate processes within the organization. The goal is to eliminate potential human errors.

Organization and Management of IT Security

At Adeo Datacenter, the CTO holds overall responsibility for IT security. To support security efforts, an IT Security Committee has been established, which meets regularly to review the company's security procedures.



Risk Management

Adeo Datacenter has established procedures that ensure the risks associated with the operation of the data center are minimized. Ongoing controls are performed through random checks, as well as every time existing systems are updated, or new systems are implemented.

The CEO is responsible for continuous risk assessment, which is approved and anchored in the management.

IT Security Management

The daily responsibility for IT security is handled by the members of the IT Security Committee. This ensures that requirements and frameworks are adhered to. The Security Committee works based on the applicable security policies.

Adeo Datacenter aims to deliver a stable and secure data center solution to its customers, and based on this objective, as many procedures as possible are automated, and checklists have been developed for manual processes. The goal is to ensure consistent delivery to customers and partners.

The security policy applies to all employees and deliveries.

If errors occur in the operational environment, they are immediately rectified. The IT Security Committee then reviews the error to prevent it from happening again. An incident report is created, which aims to inform customers and serve as a basis for knowledge sharing with employees. All network devices are registered in Adeo Datacenter's DCIM system (Data Center Information Management), and all system changes are recorded therein. Configuration files for network devices (firewalls, routers, switches, etc.) are stored in Adeo Datacenter's documentation system.

Adeo Datacenter continuously makes improvements to both policies, procedures, and operational operations.

HR, Employees, and Training

The hiring of employees and the establishment of cooperation agreements with external parties follow established procedures to ensure that the right person is hired based on background and competencies. Everyone is given a specific role and responsibility description, so they are aware of their duties.

General terms of employment, including confidentiality regarding customers and Adeo Datacenter, are outlined in each employee's employment contract. The contract also includes the employees' obligation to adhere to the applicable policies and procedures.

Employees are a crucial asset in a data center, and therefore Adeo Datacenter works proactively to ensure that all employees have the appropriate qualifications, certifications, and training. Employees' knowledge and competencies are continuously maintained through courses, both domestically and abroad.

Similarly, employees are informed when internal security procedures/policies are updated, ensuring everyone is always up to date.

Conditions regarding the termination of employment are described in each employee's employment contract. The relevant exit controls (access to systems, premises, etc.) and processes are handled by the employee's manager.

Asset Management

At Adeo Datacenter, all equipment, including servers, racks, network devices, etc., is individually registered to provide an easy overview of the equipment. Since we have a large and highly redundant network with many systems and customers connected, we have developed a special naming convention to ensure an easy understanding of the location and usage within the network.

User Management / Access Security

As part of the IT policy, Adeo Datacenter has clear procedures for granting access to the physical data center and the network. Only authorized users are granted access to the halls and systems.

Customers with access to Adeo Datacenter's halls are issued a PIN code and an individual access token. To receive an access token, the person must present a valid passport or driver's license.

Adeo Datacenter's own employees are registered only with authorization from the CTO.

Employees and customers who no longer require access must be reported to Adeo Datacenter NOC, which ensures that access is immediately revoked for the user and that accounts are deactivated.

Physical Security

<u>Hardware</u>

The hardware (racks, servers, etc.) in Adeo Datacenter is supplied by the best and most recognized manufacturers in the market, including Brocade, HP, MikroTIK, and Fortigate. Adeo Datacenter follows the supplier's guidelines for equipment maintenance. All equipment in the data center is owned by Adeo Datacenter, giving us full control. Internet connections are redundant to ensure stable operation for our customers.

Access Control

All access to the data center is secured with RFID cards, and all accesses are logged in a separate access system (for 5 years). The center is built with 5 separate halls and also has separate areas for emergency power systems, storage, and fire extinguishing equipment. All access is under 24/7/365 video surveillance.

Power Supply

The power supply in the data center is secured by an UPS emergency power system, which is taken over by a diesel generator in the event of a prolonged power outage, ensuring operations can continue if city power is lost.

Transient-protected power distribution boards in the data center protect against external electrical surges, such as lightning strikes.

Fire Safety

If smoke is detected in any hall, the Fire-eater system is automatically triggered. The fire suppression system alarms the mandatory control center, and security is automatically notified.

Cooling

An N+1 redundant cooling system has been installed in the data center. If the primary system fails, the additional system takes over. The redundant system is a traditional free cooling system consisting of three (3) cooling towers.

Location

To prevent flooding, the data center is located in an area with good drainage conditions, including a diversion channel on adjacent land where surface water can be directed away. The diversion channels are maintained by the municipality to ensure free flow. According to the Geodata Agency's drainage map, the data center is not at risk from extreme rainfall, and to our knowledge, there has never been a flood at the property.

Logging and Monitoring

Adeo Datacenter monitors all central systems and logs traffic, as well as patterns, for troubleshooting purposes in the systems.

Patch Management / Change Management

Adeo Datacenter will patch the infrastructure and ensure that security vulnerabilities are closed immediately. Changes are documented and logged in the documentation system. The systems offered to customers are handled in the same way as the rest of the infrastructure. Regular updates are first tested in our laboratory setup before being implemented on production systems.

Management of IT Security Incidents

If faults or weaknesses are detected in Adeo Datacenter's systems, they are corrected as quickly as possible to avoid unnecessary burden on customers. Additionally, faults and weaknesses are continuously reported to management so that necessary changes can be implemented and similar future incidents can be avoided.

Vendor Relationships

If vendors are granted access to the data center or systems, a signed NDA is in place. The IT Security Committee maintains a vendor overview containing access information.

Emergency Management

Adeo Datacenter's contingency plan outlines how a failure should be handled, including which systems and in what order operations should be restored. In the event of severe errors or outages, all key employees are informed about the problem and how it has been handled and resolved.

In the case of a total loss of one or more server rooms, a plan has been developed for how restoration should proceed and how backups can be recovered.

Significant Change in IT Security

There have been no significant changes during the reporting period.

Customer Responsibilities (Complementary Controls by Customers)

The current description covers standard agreements and does not include individual customer agreements. The customer is responsible for the systems they operate through Adeo Datacenter's facilities and must ensure the necessary controls are in place for operations.

The customer is responsible for ensuring that their own connections are functional and secured at a responsible level. Adeo Datacenter has a general contingency plan that covers the specific activities involved in restoring the datacenter and services. If the individual customer has an extended need, a separate plan can be developed.

3: Independent service auditor's assurance report on the description, design and operating effectiveness of controls

To: ADEO Datacenter ADEO Datacenter ApS's customers and their auditors

Scope

We have been engaged to provide assurance about Adeo Datacenter ApS's description in section 2 of its IT general controls in relation to Adeo Datacenter ApS's development and operating services which has processed customers' transactions throughout the period from 1 January 2024 to 31 December 2024 and about the design and operating effectiveness of controls related to the control objectives stated in the description.

Adeo Datacenter ApS' responsibilities

Adeo Datacenter ApS is responsible for: preparing the description and accompanying statement in section 2, including the completeness, accuracy and method of presentation of the description and statement in section 1; providing the services covered by the description; stating the control objectives and designing, implementing and effectively operating controls to achieve the stated control objectives.

Service auditor's independence and quality control

We have complied with the independence and other ethical requirements in the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct, as well as ethical requirements applicable in Denmark. Our firm applies International Standard on Quality Management 1, ISQM 1, which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on Adeo Datacenter ApS' description and on the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures.

We conducted our engagement in accordance with ISAE 3402-II, "Assurance Reports on Controls at a Service Organization", issued by the International Auditing and Assurance Standards Board, and additional requirements applicable in Denmark. This 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 effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its development and operating services and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of risks that the description is not fairly presented, and that controls are not suitably

designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified and described by EG Danmark A/S in the Management's statement section.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of controls at Adeo Datacenter ApS

Adeo Datacenter ApS' 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 Adeo Datacenter ApS' development and operating services that the individual customer may consider important in its particular circumstances. Also, because of their nature, controls at a service organization may not prevent or detect all errors or omissions in processing or reporting transactions. Furthermore, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

Our opinion has been formed based on the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the Management's statement section. In our opinion, in all materiel respects:

a) The description fairly presents how IT general controls in relation Adeo Datacenter ApS' development and operating services were designed and implemented throughout the period from 1 January 2024 to 31 December 2024;
b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 January 2024 to 31 December 2024; and
c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 January 2024 to 31 December 2024.

We must note that for individual customers there may be specific conditions which mean that the general conclusion is not comprehensive. If it has been agreed between the customer and Adeo Datacenter ApS that a specific statement regarding the customer's contract will be drawn up, the conditions will appear from this.

Description of tests of controls

The specific controls tested and the nature, timing and results of these tests are listed in section 4.

Intended users and purpose

This report and the description of tests of controls in section 4 are intended only for customers who have used Adeo Datacenter ApS' development and operating services and their auditors who have a sufficient understanding to consider it along with other information, including information about controls operated by the customers themselves, in assessing the risks of material misstatement in their financial statements.

Roskilde, 31. oktober 2025

Algade Revision
Registreret revisionsanpartsselskab
CVR 35 66 39 16

_____
Mick Andersen
Registreret revisor, FSR – danske revisorer
MNE: mne41282

4: Control objectives, control activity, test and test results

The following overview has been created to provide an understanding of the effectiveness of the controls implemented by Adeo Datacenter ApS. Our test of functionality has covered the controls that we deemed necessary to achieve a high level of assurance that the stated control objectives were met during the period from 1 January 2024 to 31 December 2024.

Therefore, we have not necessarily tested all the controls mentioned by Adeo Datacenter ApS in its description in section 2.

Controls performed at Adeo Datacenter ApS' customers, moreover, are not covered by our statement, as the customers' own auditors must conduct this review and assessment.

We have conducted our tests of the controls at Adeo Datacenter ApS through the following actions:

Method	General description
Enquiry	Enquiries to/interview with relevant staff at ADEO DC. Enquiries have included how control measures are performed.
Observation	We have observed the performance of the control.
Inspection	Reading of documents and reports containing information about execution of the control. This includes reading and deciding about reports and other documentation to assess, whether it can be expected that the design of specific control measures will be efficient, if implemented. Furthermore, it is assessed whether control measures are monitored and controlled sufficiently and with appropriate intervals.
Re-performing control procedures	Repeated the relevant control measure. We have repeated the performance of the control to verify that the control measure works as assumed.

The description and results of our test based on the tested controls are presented in the following tables. To the extent that we have identified significant weaknesses in the control environment or deviations from it, we have noted these.

Monitoring			
No.	Control objective	Audit test	Test result
1.1	Adeo DC monitors datacenter solutions using remote monitoring, which includes monitoring alarms related to temperature, fire, water, access conditions, etc.	We have inquired about the procedures regarding monitoring and incident handling, including the registration of information. We have observed that Adeo DC monitors cables, housing facilities, and circuits using remote monitoring.	No comments.

Access control			
No.	Control objective	Audit test	Test result
1.2	The facilities of the data center solutions are equipped with access control systems to ensure that only authorized and approved employees and designated persons from customers have access to these facilities. Authorization, issuance, and deactivation of access media follow Adeo DC's quality process for this purpose.	We have inspected the procedure regarding access control in the data centers. Through random sampling, we observed that access cards are required to gain entry to the data centers. We have observed that access activities are recorded and monitored. We have also inspected that there is an ongoing review of both internal and external user access.	No comments.

Preventive maintenance

No.	Control objective	Audit test	Test result
1.3	Adeo DC conducts weekly inspections of the data center facilities. The results of these inspections are documented in completed forms.	We have inquired about procedures for preventive inspections. We have randomly inspected to verify that weekly checks are conducted in the areas of power, climate, fire safety, and general maintenance, and that these are documented in completed forms.	No comments.

Physical security

No.	Control objective	Audit test	Test result
1.4	Adeo DC complies with specified physical security requirements for data center solutions, covering the following aspects: Building, floors, climate, power, access, alarm monitoring, automatic fire suppression and cabling.	We have inquired about the procedures for compliance with physical security requirements. Through random sampling, we have observed that the data center meets the requirements.	No comments.

Contingency Plan			
No..	Control objective	Audit test	Test result
1.5	Adeo DC's contingency plan is continuously tested. The results of the tests are documented.	We inquired about procedures related to contingency plans and their testing. We have inspected that contingency drills have been conducted as planned and documented.	No comments.

Human Security			
No.	Control objective	Audit test	Test result
1.6	Adeo DC identifies all customers via passport or driver's license, as well as the signing of relevant materials provided. Adeo DC has processes for the return of Adeo DC's property, as well as the closure of all access upon employee departures.	We have inspected that Adeo DC performs checks on customers, as well as procedures for disabling access, etc.	No comments.

Compliance

No.	Control objective	Audit test	Test result
1.7	The purpose is to ensure that information security is implemented and operated in accordance with the organization's policies and procedures.	We have inquired about the periodic independent evaluation of IT security and the monitoring of compliance with policies and technical configurations.	No comments.

Remote Access

No.	Control objective	Audit test	Test result
1.8	Two-factor authentication access is used to ensure that employees have been approved to gain access.	We have inspected that procedures exist to ensure that two-factor authentication is used to sensitive and critical systems in Adeo DC's infrastructure.	No comments.

Vulnerability Management

No.	Control objective	Audit test	Test result
1.9	Continually vulnerability scanning of critical infrastructure is performed to reduce the risk of getting compromised.	We have inspected that procedures exist for regular testing including various scans and penetration tests.	No comments.

Secure Areas			
No.	Control objective	Audit test	Test result
1.10	All critical IT-infrastructure to operate customers cloud services, are placed in a secure and private data hall within the data center.	We have inspected that procedures exist to ensure that only authorized persons can gain physical access to the areas with critical and sensitive hardware.	No comments.

Dette dokument er underskrevet af nedenstående parter, der med deres underskrift har bekræftet dokumentets indhold samt alle datoer i dokumentet.

Mikkel Emmerik

Navn returneret af MitId: Mikkel Emmerik
DirektÃ¸r
ID: 0d5d53a0-973b-4ec0-9e11-55f81eeef4a0
IP-adresse: 172.225.69.76:42695:42695
Dato for underskrift: 31-10-2025 15:04:09 CET (+01:00)
Underskrevet med MitID

Mick Andersen

Navn returneret af MitId: Mick Berthou Hagberg Andersen
Revisor
ID: 46c4064e-6645-477c-8388-12fa167058cd
IP-adresse: 185.152.200.72:13567:13567
CVR-match med MitId
Dato for underskrift: 31-10-2025 15:05:15 CET (+01:00)
Underskrevet med MitID Erhverv