INDEPENDENT AUDITOR'S ISAE 3402 ASSURANCE REPORT FOR THE PERIOD FROM 1 APRIL 2024 TO 31 MARCH 2025 ON THE DESCRIPTION OF THE EMENTO PRODUCT SUITE AND THE RELATING CONTROLS, THEIR DESIGN AND OPERATING EFFECTIVENESS

Emento A/S

CONTENTS

1. AUDITOR'S REPORT 2

2. EMENTO A/S STATEMENT 5

3. EMENTO A/S' DESCRIPTION OF THE EMENTO PRODUCT SUITE 7

General description of Emento A/S 7

Description of The Emento Product Suite 7

Risk management of The Emento Product Suite 7

Control framework, control structure and criteria for control implementation 7

Changes during the period from 1 April 2024 to 31 March 2025 15

Complementary controls with the customer 15

4. CONTROL OBJECTIVES, CONTROLS, TEST AND RESULTS OF TESTS 16

A.5: Information security policies 18

A.6: Organisation of information security and internal organisation 19

A.7: Employee safety 22

A.8: Asset Management 25

A.9: Access Management 27

A.10: Encryption 31

A.11: Physical protection and environmental protection 32

A.12: Operational reliability 36

A.13: Communication security 41

A.14: Acquisition, development and maintenance of systems 43

A.15: Supplier relations 45

A.16: Management of information security incidents 47

A.17: Information security aspects of emergency, emergency and re-establishment management 49

A.18: Compliance 50

1. AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT FOR THE PERIOD FROM 1 APRIL 2024 TO 31 MARCH 2025 ON THE DESCRIPTION OF THE EMENTO PRODUCT SUITE AND THE RELATING CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS

To: The Management in Emento A/S
Emento A/S' customers and their auditors

Scope

We have been engaged to report on Emento A/S (the service provider) description in section 3 of The Emento Product Suite and related controls, and on the design and operation of controls related to the control objectives stated in the description, throughout the period from 1 April 2024 to 31 March 2025.

The Service Provider's Responsibilities

The service provider is responsible for preparing the description and accompanying statement in section 2, including the completeness, accuracy, and method of presentation of the description and the statement.

The service provider is responsible for providing the services covered by the description; stating the control objectives; and identifying the risks threatening achievement of the control objectives; designing and implementing effectively operating controls to achieve the stated control objectives.

Auditor's Independence and Quality Assurance

We have complied with the requirements of independence and other ethical requirements of the International Ethics Standards Board of Auditors' International Guidelines on the Conduct of Auditors (IESBA Code), which are based on the fundamental principles of integrity, objectivity, professional competence, and due diligence, confidentiality, and professional conduct, as well as ethical requirements applicable in Denmark.

BDO Statsautoriseret revisionsaktieselskab applies International Standard on Quality Management, 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.

Auditor's Responsibilities

Our responsibility is, on the basis of our actions, to express a conclusion about the service provider's description as well as about the design and operational efficiency of controls related to the control objectives set out in this description.

We have performed our work in accordance with the International Standard on Assurance Engagements 3402 on declaration duties with security checks at a service organisation. This standard requires that we plan and carry out our actions in order to obtain a high degree of certainty as to whether the description is correct in all material respects and whether the controls in all essential respects are appropriately designed and have operated effectively.

A declaration task with certainty to provide a statement about the description, design, and operational efficiency of controls at a service provider includes performing actions to obtain evidence of the information in the service provider's description as well as of the controls' design and operational efficiency. The actions chosen depends on the assessment of the service provider's auditor, including the assessment of the risks

that the description is not accurate and that the controls are not appropriately designed or do not operate effectively. Our actions have included tests of the operational efficiency of such controls, which we consider necessary to provide a high degree of assurance that the control objectives set out in the description were achieved. A statement of assurance with certainty of this type further includes an assessment of the overall presentation of the description, the appropriateness of the control objectives set out therein and the appropriateness of the criteria specified and described by the service provider in section 2.

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

Limitations of Controls at a Service Organisation

The service organisation's description is prepared to meet the common needs of a wide range of customers and their auditors and may not, therefore, include every aspect of The Emento Product Suite that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in service providers statement in section 2. In our opinion, in all material respects:

a. The description of The Emento Product Suite and related controls, as designed and implemented throughout the period from 1 April 2024 to 31 March 2025 is in all material aspects, accurate and

b. The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 April 2024 to 31 March 2025; 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 April 2024 to 31 March 2025.

Description of Tests of Controls

The specific controls tested, and results of those tests are listed in section 4.

Intended Users and Purpose

This report is intended only for customers, which have used the service providers The Emento Product Suite, and their auditors who have a sufficient understanding to consider it, along with other information about controls operated by the customer themselves when obtaining an understanding of customers' information systems relevant to financial reporting.

Copenhagen, 1 May 2025

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, State Authorised Public Accountant

Mikkel Jon Larssen
Partner, Head of Risk Assurance, CISA, CRISC

2. EMENTO A/S STATEMENT

Emento A/S has prepared the following descriptions of controls relating to the Emento Product Suite to the company's customers.

The description has been prepared for Emento A/S' customers and their auditors who have a sufficient understanding to consider the Emento Product Suite, along with other information, including information about controls operated by the customers themselves, when assessing the risks of material misstatements of customers' financial statements.

Emento uses service subcontractors. The relevant control measures and associated controls of these service subcontractors are not included in the accompanying description.

Emento confirms that the accompanying description in section 3 fairly presents controls in relation to the Emento Product Suite and associated controls throughout the period from 1 April 2024 to 31 March 2025. The criteria used in making this statement were that the accompanying description:

1. Explains the Emento Product Suite, and how associated controls were designed and implemented, including explaining:
    - The services provided, regarding the handled groups of transactions, when it is relevant.
    - The processes in both IT and manual systems that are used to initiate the records, process and if necessary, correct the transactions and transfer these to the reports prepared for customers.
    - The associated accounting records, underlying information and specific accounts used to initiate, record, process, and report transactions, including the correction of incorrect information, and how the information is transferred to the reports prepared for customers.
    - How the system handles other significant events and conditions than transactions.
    - The process used to make reports to customers.
    - Relevant control objectives and controls designed to achieve those objectives.
    - Controls that what we have assumed would be implemented by the user companies with reference to the design of the system and which, if necessary to achieve the control objectives stated in the description, are identified in the description along with the specific control objectives we cannot reach ourselves.
    - Other aspects of our control environment, risk assessment process, information system (including the associated business processes) and communication, control activities and monitoring controls that have been relevant to the processing and reporting of customer transactions.
2. Includes relevant details of changes to the controls relating to the service providers The Emento Product Suite during the period from 1 April 2024 to 31 March 2025.
3. Does not omit or distort information relevant to the scope of the controls described relating to the Emento Product Suite 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 the Emento Product Suite that the individual customer may consider of importance to their special environment.

Emento A/S confirms that controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 April 2024 to 31 March 2025. The criteria we used in making this statement were that:

1. The risks that threatened achievement of the control objectives stated in the description were identified.

2. The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

3. The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 April 2024 to 31 March 2025.

Aarhus, 1 May 2025

Ementa A/S

Allan Juhl
CEO

3. EMENTO A/S' DESCRIPTION OF THE EMENTO PRODUCT SUITE

GENERAL DESCRIPTION OF EMENTO A/S

This description is prepared for the purpose of reporting on the IT general controls that Emento applies to support and safeguard provision of IT operations to its customers. The description focuses on business-related control objectives and processes implemented to safeguard Emento's provision of IT operations.

DESCRIPTION OF THE EMENTO PRODUCT SUITE

The Emento Product Suite is a service for ongoing communication between patient/citizen and/or hospital/municipality.

The platform consists of an app aimed at the citizen/patient and web access aimed at the staff. The staff define a process which guides and informs the citizen/patient continuously via an app.

Through the app, the citizen/patient can send messages to the unit and the staff can respond when it suits. This reduces disruptive phone calls. Staff gain knowledge of the citizen/patient's interaction with the app and can use this to reduce unforeseen no-shows and cancellations.

To support the creation of good pathways and the rapid translation of learning into new content or workflows, Emento has developed a range of support products to enable staff to organise or correct pathway structure and content themselves.

The app can be used for several care guides from different data controllers. The citizen's profile is the same for all care guides. Therefore, Emento is the data controller of the citizen profile, and the sender of the care guide is the data controller of data related to the care guides.

Emento hosts, operates, maintains, and supports the Emento Product Suite.

A lighter version of the Emento Product Suite without MitID validation and the possibility to immediately delete a citizen profile is sold under the brand _Guide. This solution is hosted at Hetzner.

RISK MANAGEMENT OF THE EMENTO PRODUCT SUITE

An annual risk assessment is carried out and input for this assessment is obtained from all levels of the organisation.

Risk assessments are based on the implementation guidelines in the international standard ISO 27002.

Emento has a process to continuously identify, assess, and act on risks that may impact the business or the rights of data subjects. All risks are assessed against well-defined criteria of likelihood and impact. This assessment, as well as the decision to respond, is documented in a risk analysis that reflects the reality of our business at all times.

Based on a risk assessment, the day-to-day Management of Emento decides whether an identified risk can be accepted, is to be reduced or whether insurance is required, based on selected risks.

This report includes solely controls and control objectives for processes and controls that are managed by Emento and, thus, it does not include controls or control objectives that are managed by sub-organisations.

CONTROL FRAMEWORK, CONTROL STRUCTURE AND CRITERIA FOR CONTROL IMPLEMENTATION

Emento wishes to maintain and continuously develop a level of IT security in line with the requirements outlined in ISO 27001 - Information Security. The requirements are tightened in well-defined areas where there are special legal requirements, contractual conditions or possibly special risk (identified by a risk assessment).

An effective defense against IT security threats must be created in order to best safeguard Emento's image and the security and working conditions of its employees. The protection must address natural as well as technical and man-made threats. All persons are considered to be a possible cause of a security breach, i.e. no group of people should be above the security rules.

The objectives are therefore to ensure:

1. AVAILABILITY - by achieving high reliability with high uptime percentages and minimised risk of major outages and data loss.
2. INTEGRITY - by achieving correct functioning of the systems with minimised risk of manipulation and errors in both data and systems.
3. CONFIDENTIALITY – by achieving confidentiality in the processing, transmission and storage of data.
4. AUTHENTICITY - by achieving mutual security around the parties involved.
5. INDEPENDENCE - by obtaining a guarantee of mutual and documentable contact.

The determination of criteria and scope of control implementation at Emento is based on the ISO 27002:2013 framework for management of information security. The following control areas in ISO 27002 were assessed:

- A.5. Information security policy
- A.6. Organisation of information security
- A.7. Human resource security
- A.8. Asset management
- A.9. Access management
- A.10. Cryptography
- A.11. Physical and environmental security
- A.12. Operations security
- A.13. Communications security
- A.14. Acquisition, development and maintenance of systems
- A.15. Supplier relationships
- A.16. Information security incident management
- A.17. Information security aspects of contingency, disaster recovery and restore management
- A.18. Compliance

Implemented control environment
The implemented controls are based on the services provided by Emento to customers and include control areas and control activities within operation and hosting. All of the above areas are described in detail in the following in separate paragraphs, and the described control objectives and controls for those areas in the paragraph on control objectives, controls, tests and result of tests are an integral part of the description.

A.5 Information security policy
Emento has drawn up a formal information security policy with accompanying instructions which have been incorporated in an information security handbook. One of the instructions in the handbook describes Emento’s policy for managing information which provides instructions for the management of information and data in the daily work. It is provided in connection with employment and all employees are also required to ensure that they are updated on a regular basis in relation to the information security policy and the related procedures,

guidelines and handbooks. Policies, procedures, guidelines and handbooks are approved annually or when material changes are made. Finally, our suppliers/business partners are made familiar with the information security policy when obtaining non-disclosure agreements. The information security policy is reassessed annually by Management.

A.6 Organisation of information security

Emento has implemented controls to ensure general management of the information security, including a delegation of responsibilities and managing material risks in accordance with the requirements of the Company's Management.

Management's obligations in relation to information security

Management takes an active part in the IT security in the organisation. The formal responsibility, including approval of the information security policy, is also that of the CEO.

Coordination of the information security

Activities to safeguard the information security are considered in an organisational security and data protection committee with participants from all relevant departments.

Placing of responsibility for information security

All areas of responsibility for the IT security are described in Emento's security policy which clearly describes where the responsibility is placed in relation to information security and the contingency planning.

Placing of responsibility for data protection

The business' CEO is always responsible for the data protection. The CEO manages together with the security and data protection committee the operational responsibility for complying with personal data protection, internally and in relation to customer data. Management obtains advice on questions related to data protection from the appointed DPO.

Mobile data processing and communication

Emento's mobile device and teleworking policy sets out rules for use of mobile equipment outside the company. Only equipment, which complies with Emento's information security policy relating to protection against malicious code, can access the network from the outside and exclusively via VPN.

All remote access to production environments can solely be performed via our authorised PCs. Access from home workplace is secured via encrypted VPN connection, which requires machine validation and explicit user access.

Authentification of users on external connections

All access to our network, including external users, is authorised by our formal Access Management procedure, described in our Access Control Policy.

Non-approved user equipment

Guest equipment and non-approved equipment, for example mobile phones, can solely be connected to a separate guest network.

A.7 Human resource security

Emento has implemented controls to ensure that employees are qualified and conscious of their tasks and responsibilities in relation to information security.

For the purpose of employment at Emento, applicants must provide an unblemished criminal record at the second job interview.

Management's responsibility

As regards employees, they commit themselves, at their employment, to comply with the company's policies, including the security policy.

Awareness of information security and data protection, education and training
As regards employees, they are informed of all material changes to applicable policies and relevant procedures. This is done partly at the monthly meetings in the Security and Data Protection Committee and partly at staff meetings.

The employees are currently informed of personal data protection, so that there is a constant awareness of how employees manage the work with personally identifiable data, their own as well as the customers' data.

Roles and responsibilities
The responsibilities of the employees follow their place in the organisation. The responsibilities of all staff in relation to IT security are described in the staff handbook, and where an increased responsibility applies this is described in the information security policy.

Non-disclosure agreements
Confidentiality is part of the employment contracts. For a few customers there are special non-disclosure and confidentiality agreements and other security provisions for the employees working with the customer. Moreover, an overview has been prepared of all laws, requirements and security circulars that Emento must comply with. The list is reviewed annually by the administrative manager and the necessary renewals are made, if relevant.

Obligations relating to departures
General employment conditions, including conditions in relation to end of employment, are described in the employee's employment contract and confidentiality declaration. Moreover, there is a formal procedure for departure which must be followed by the immediate manager. The CEO is the ultimate responsible in this respect.

Return of equipment
All employees are to return all received material when the employment contract ends. This is done through a workflow carried out by the responsible manager.

Closing of access rights
Emento's formal HR procedures ensure that all rights and physical access are withdrawn when an employment ends. This is done through a workflow carried out by the responsible manager. Accesses are reviewed every six months.

Sanctions relating to breach of the information security
In addition to common employment law provisions, the information security policy specifies sanctions. The workplace is subject to Emento's security routines which must not be broken. If this happens, management will handle the situation case-by-case and may initiate sanctions.

A.8 Asset management

Emento has implemented controls to ensure achievement and maintenance of suitable protection of the organisation's equipment.

Registration of equipment
Relevant equipment, which is utilised, is registered in Emento in service desk system, in which all changes are also registered. Moreover, there is an updated list of all authorised, mobile units. Non-utilised equipment is stated on an asset list and updated.

Accepted use of equipment

The employees' use of IT equipment and data is subject to fixed guidelines, defined in Emento's information security handbook.

Management of portable media
The rules for use of portable media are contained in the classification system described in the mobile device and teleworking policy.

Procedures for information management
All processing of data follows the guidelines set out in the information handling policy for Emento.

The guidelines for processing of personally identifiable data comply with the guidelines set out in the information security policy. The information security policy sets out the guidelines for sanctions in case policies, procedures or handbooks are not complied with.

A.9 Access management

Emento has implemented controls to ensure that access to systems and data are granted through a documented process in accordance with a relevant work-related need and is closed down when the relevant access is no longer necessary.

Procedure for access control
As a supplement to our security policy, Emento has a formal policy and procedure for access management.

Guidelines for use of network services
All user rights, including access to network, drives and applications, are determined on the basis of their function.

User creation
Emento has procedures for creation and closing down of users based on employment checklist.

Extended rights
All rights are managed on the basis of the employees' roles and are checked regularly in our access management system. Extension of standard rights follows our formal access management procedure.

Management of password
Granting of passwords is subject to a number of rules which are set out in our information security policy and enforced by 1Password access groups.

Reassessment of user access rights
All accesses and rights are reviewed periodically by the security and data protection committee.

User identification and authentication
Emento has separate admin profiles for all operational staff in the systems where this is technically possible. All password validation is made by 1Password which manages validation of the individual logins.

A.10 Cryptography

Emento has implemented controls to ensure correct and effective use of cryptography to protect confidentiality, authenticity and/or integrity of data.

A.11 Physical and environment security

Emento has implemented controls to ensure that IT equipment is properly protected against 11uthorized 11d physical access and environmental incidents.

Physical access control

Emento premises have access control in the form of a required personal key ring to ensure that only authorized staff have access. Only Emento employees receive a key ring. If suppliers, consultants or other external parties are to have access, this is only possible together with authorized personnel. Agreements have been made for logical access control to be carried out by team.blue and Hetzner.

Safeguarding of offices, premises and facilities
Emento premises have access control in the form of a required personal key ring to ensure that only 12uthorized staff have access.

Protection against physical external threats
We refer to separate ISAE 3402 report and ISO 27001-certifcation on the description of controls, their design and operating effectiveness relating to team.blue and Hetzner.

Public areas, loading and unloading areas
Public access is only possible in the reception area. All other access is possible only together with authorized staff. Other entrance doors require a personal key ring. The unloading area at the ground floor is also separated by both a separate door.

Storing of equipment and protection of equipment
The critical equipment is placed in the server room to which only Emento staff have access. Critical equipment is stored in an environmentally secured and locked cabinet which only designated technical staff has access to.

A.12 Operations security

Emento has implemented controls to ensure that operation of servers and key systems is carried out in a structured and secure manner.

Documented operating procedures
All operating procedures are available in Emento's document management system and enforced by dev-ops scripts and platforms.

Safeguarding of systems documentation
Emento keeps the systems documentation centrally in our document management system which can solely be accessed by authorised staff.

Control of procedures for changes
We have a formal procedure for change management.

Management of capacity
Monitoring of capacity has been implemented in relation to internet, network, servers, disk space and log files. Emento receives reporting from the monitoring system and other tools which are used in the planning of purchase of additional capacity. Data from monitoring are registered and evaluated currently.

Backup of information
Backup is taken of all important data according to customer agreements made. Failed backups are logged and monitored through Emento's monitoring system. Restore test for the customer is performed only when a specific agreement exists between the customer and Emento. General test of backup is performed annually.

Control of malicious code
All registered servers in Emento's infrastructure are installed, updated and patched automatically according to Best Practice within the area. All workstations in Emento are updated according to Best Practice with antivirus software.

Audit log

User transactions, exceptions and security incidents are logged, and the log is stored according to the retention periods agreed with the customer.

Use of monitoring systems
Emento has implemented internal procedures to ensure that alarms are addressed in order to respond to relevant incidents and act accordingly. All relevant alarms are shown on a big screen within normal working hours and to the on-duty officer during on-duty periods. All alarms are reviewed daily.

Incident logging
All incidents are registered in Emento's IT Service Management System. Incidents concerning breach in relation to the processing of personal data are always marked, so that they can rapidly be identified and dealt with by Emento's DPO. Incident logs are created and kept for incidents concerning processing of personal data and incidents that have had a significant impact on the customers experience of the service.

Logging of administrator and operator
System administrators' actions are logged automatically.

Logging of errors
Monitoring has been set up for the purpose of future analysis of errors and incidents.

A.13 Communications security

Emento has implemented controls to ensure that operation of material infrastructure components is carried out in a structured and secure manner.

Network controls
Emento has written procedures for configuration of firewalls, routers and switches, which are solely carried out by the operations department.

Security services on the network
Access to Emento's systems for our customers goes through public networks where access is via VPN and firewall. Access and communication between our servers and the internet goes through our centrally managed firewall, where logging has been set up. All incoming network traffic goes through our firewalls. Only approved network traffic is allowed through the firewall.

Policies and procedures for data exchange
All data exchanges are as a minimum encrypted, meaning that they go via a VPN encryption.

Control of network connections
Customer networks are limited by the VLAN and Access rules in our Core router/firewall. It is solely approved Emento personnel that can access the different customers' VLANs.

A.14 Acquisition, development and maintenance of systems

Emento has implemented controls to ensure that servers and relevant infrastructure components are updated and maintained as necessary and that this is done in a structured process.

Change management
Emento has a formal Change Management procedure to ensure that systems are reassessed and tested in connection with major changes and follows the process in our service desk system in the form of formalised workflows. Security patches are installed automatically, and all other service updates are installed by Emento at the release of new Emento Suites.

Control of technical vulnerabilities
Scanning for updates to systems is done by means of linux unnatended_upgrades. Hereafter, Emento's formal procedure for patching is followed.

A.15 Supplier relationships

Emento uses team.blue and Hetzner as sub-supplier of physical security and monitoring. The service provided by team.blue and includes:

- Monitoring of the physical location
- On-call services in case of alarm

Management of security in agreements with third party
If the sub-suppliers are an integral part of our services, we inspect the controls implemented by the supplier by obtaining an ISAE 3402 auditor's report or similar documentation.

To the extent that Emento's sub-suppliers store or otherwise manage personal data on behalf of Emento's customers in the course of the sub-supplier's provision of services to Emento, the sub-supplier acts as data processor solely according to instructions from Emento and Emento's customer. Thus, Emento's sub-suppliers commit themselves to take the necessary technical and organisational security measures to ensure that personal data are not accidentally or illegally destroyed, lost or impaired, and that they are not disclosed to unauthorised parties, misused or otherwise processed in violation of data protection legislation.

A.16 Information security incident management

Emento has established controls and guidelines which ensure that incidents are dealt with in time and that there is a follow-up on the incidents.

All incidents, including security incidents, follow our formal Incident Management procedure.

Emento has implemented procedures for documentation of all breaches of the management of personal data. Problem Management, which includes identification of the "root cause" of the breach of applicable guidelines for the management of personal data, preventive and corrective measures. All procedures are available to employees with a functional need.

A.17 Information security aspects of contingency, disaster recovery and restore management

Emento has prepared a contingency plan which is updated as required.

Information security integrated in the contingency plan
Emento has a formal contingency plan in which information security is incorporated.

Development and implementation of contingency plans which include information security
We have developed contingency plans to maintain or restore operations and ensure access to data at the required level and within acceptable time after failure or outage of critical business processes.

Responsibilities and guidelines
Roles and responsibilities are defined in the contingency plan.

Contingency plan
Emento assesses risks regularly, and the contingency plan is updated to the existing risk exposure at least once a year in connection with Management's review and approval of the security policy.

Testing, maintenance and reassessment of contingency plans
The contingency plan is tested annually to ensure that it is applicable, sufficient and effective.

A. 18 Compliance with laws and internal policies

The Service Provider has an overview of current legislation, contractual requirements, best practices and internal policies that the Service Provider should comply with.

A written procedure defines how to identify new compliance requirements. All data processing agreements,

customer contracts and supplier contracts has been reviewed. Changes to supplier contracts and DBAs are reviewed each year.

The Service Provider oversees compliance with the requirements specified in suppliers and data processors contract and Data Processing Agreements on a regular basis.

All new suppliers and data processors have to go through the approval process described in the IT Security Handbook.

The Service Provider has an overview of all – not approved and approved - systems and services. An MDM system has been installed on all workstations.

CHANGES DURING THE PERIOD FROM 1 APRIL 2024 TO 31 MARCH 2025

Emento A/S has not made significant changes of the The Emento Product Suite and the relating technical and organisational security measures and other controls during the period from 1 April 2024 to 31 March 2025.

COMPLEMENTARY CONTROLS WITH THE CUSTOMER

The customer is obligated to implement the following technical and organisational security measures and other controls to reach the control objectives and thereby comply with the data protection legislation:

- The customer is responsible for ensuring that the administrators' use of The Emento Product Suite is in accordance with relevant legislation.
- The customer controls the user privileges in The Emento Product Suite, including who are allocated administrator access and which rights the individual administrators are allocated.

4. CONTROL OBJECTIVES, CONTROLS, TEST AND RESULTS OF TESTS

Objective and scope

BDO has carried out the work in accordance with ISAE 3402 on assurance engagements relating to controls at a service organisation.

BDO has performed procedures to obtain evidence of the information in Emento A/S description of the Emento Product Suite and the design and the operating effectiveness of these controls. The procedures performed depend on BDO's assessment, including the assessment of the risks that the description is not fairly presented and that the controls are not suitably designed or operating effectively.

BDO's test of the design and operating effectiveness of controls has included the control objectives and related control activities selected by Emento A/S, and which are described in the following.

In the check form, BDO has described the tests performed which were considered necessary to obtain a reasonable degree of assurance that the stated control objectives were achieved and that the related controls were suitably designed and operated effectively throughout the period from 1 April 2024 to 31 March 2025.

Test procedures

Tests of the design of technical and organisational security measures and other controls, the implementation and effectiveness hereof were performed by inquiry, inspection, observation, and re-performance.

Type	Description
Inquiry	Inquiries of relevant personnel at Emento A/S have been performed for all significant control activities. The purpose of the inquiries was to obtain knowledge and further information about implemented policies and procedures, including how the control activities are performed, and to obtain confirmed evidence of policies, procedures, and controls.
Inspection	Documents and reports, which include information about the performance of the control, have been read for the purpose of assessing the design and monitoring of the specific controls, i.e., whether the design of the controls is such that they are expected to be effective if implemented, and whether the controls are sufficiently monitored and checked at suitable intervals. Tests have been performed of significant system structures of technical platforms, databases, and network equipment to ensure that controls have been implemented, including for example assessment of logging, back-up, patch management, authorisations and access controls, data transmission, and inspection of equipment and locations.
Observation	The use and existence of specific controls have been observed, including tests to ensure that the control has been implemented.
Re-performance	Controls have been re-performed to obtain additional evidence that the controls operate as assumed.

For the services provided by Hetzner Online GmbH within hosting, we have received an ISO 27001 certification for the period 27 September 2019 to 26 September 2025 and an internal safety report signed in 2024 on technical and organisational security measures relating to operation of the hosting services.

With respect to the services provided by Team Blue A/S (ScanNet) within hosting, we have from an independent auditor received the ISAE 3402 report and ISAE 3000 GDPR report for the period 1 January to 31 December 2024.

With respect to the services provided by TwentyThree ApS within the video platform, we have from an independent auditor received the ISAE 3000 GDPR report for the period 1 January 2023 to 31 January 2024 from on technical and organisational security measures relating to operation of the video platform.

With respect to the services provided by Kontainer A/S within Digital Asset Management, we have from an independent auditor received the ISAE 3402 report for the period 1 April 2023 to 31 March 2024 on technical and organisational security measures relating to operation of Digital Asset Management.

With respect to the services provided by OnlineCity A/S within SMS gateway, we have from an independent auditor received the ISAE 3000 GDPR report for the period 1 May 2023 to 30 April 2024 on technical and organisational security measures relating to operation of the SMS gateway.

With respect to the services provided by Meedio within video consultation, we have from an independent auditor received the TÜV Certificate for the period 15 December 2023 to 15 December 2026 as well as the ISAE 3402 and the ISAE 3000 GDPR reports for the period 29 January 2023 to 29 February 2024 on technical and organisational security measures relating to operation of the video conferencing.

With respect to the services provided by SurveyXact within form creation, we have from independent auditor received the ISO 27001 Certificate for the period 26 June 2024 to 25 June 2027 and the ISAE 3000 GDPR report for the period 1 June 2023 to 31 May 2024 on technical and organisational security measures relating to operation of the form creator.

For the services provided by Digital Ocean within backup cloud hosting, we have received a SOC 2 Type 2 report for the period 1 January to 31 December 2024 and an APEC PRP certification given on 8 November 2024 on technical and organisational security measures relating to operation of the backup services.

This sub-service provider's relevant control objectives and related controls are not included in Emento A/S' description of services and relevant controls related to operation of Emento A/S' Outsourcing Services. Accordingly, we have solely assessed the report and tested the controls at Emento A/S that monitor the operating effectiveness of the sub-service provider's controls.

Result of test

The result of the test made of technical and organisational measures and other controls has resulted in the conclusions specified on the following pages.

An exception exists when:

- Technical and organisational measures and other controls have not been designed or implemented to fulfil a control objective,
- Technical and organisational measures and other controls related to a control objective are not suitably designed and implemented or did not operate effectively throughout the period.

A.5: Information security policies

Control objectives

- *To provide guidelines for and support information security in accordance with business requirements and relevant laws and regulations.*

Control activity	Test performed by BDO	Result of test
Policies for information security ▶ The service provider has developed and implemented an information security policy. ▶ The service provider has developed and implemented a policy, including a guarantee of assistance and obligation to achieve compliance with relevant requirements, laws and regulations.	We have made inquiries with relevant personnel at the service provider. We have inspected the information security policy. We have inspected that the service provider has implemented measures to ensure compliance with the information security policy.	No exceptions noted.
Review of policies for information security ▶ The service provider's information security policy is reviewed and updated at least once a year.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's annual cycle. We have inspected that the information security policy is reviewed and updated in August 2024.	No exceptions noted.

A.6: Organisation of information security and internal organisation

Control objectives

- *To establish a managerial basis to initiate and control the implementation and operation of information security in the organisation.*
- To ensure that employees and contractors understand their responsibilities and are suited to the roles for which they are intended.

Control activity	Test performed by BDO	Result of test
Roles and responsibilities ▶ The service provider has a clearly divided organisation in relation to information security and has detailed descriptions of responsibilities and roles for the individual employees.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's safety manual and information security policy. We have inspected that the TRUST group is responsible for the information security and data protection. We have observed that the top management and information security coordinator is a part of the TRUST group. We have inspected that the TRUST group has monthly meetings.	No exceptions noted.
Functional separation ▶ The conflicting functions and responsibilities of the service provider are separated, to the extent possible, considering the size of the company, to reduce the possibility of unauthorised or unintentional use, alteration or misuse of data.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's safety manual and information security policy. We have observed that the service provider has separated allocation of rights through 1Password, which assures that there are no contradicting functions and responsibilities.	No exceptions noted.
Contact with authorities ▶ The service provider keeps up to date with news from authorities.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider keeps up to date with news from authorities.	No exceptions noted.

A.6: Organisation of information security and internal organisation

Control objectives

- *To establish a managerial basis to initiate and control the implementation and operation of information security in the organisation.*
- To ensure that employees and contractors understand their responsibilities and are suited to the roles for which they are intended.

Control activity	Test performed by BDO	Result of test
Information security in project management ▶ Information security is included in project management.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider's safety manual and observed that changes require risk assessment. We have inspected that risk assessment is conducted in connection with the initiation of the change management process. We have by samples inspected that relevant changes are risk assessed.	No exceptions noted.
Mobile device policy ▶ The service provider has developed and implemented a policy and supporting security measures to manage risks to personal data arising from the use of mobile equipment.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's mobile device policy. We have observed that procedures for handling and storage of mobile equipment are presented in the mobile device policy.	No exceptions noted.
Remote workstations and remote access to systems and data ▶ All mobile devices used for work purposes must have antivirus installed and updated. ▶ Remote access to the service provider's systems and data is via an encrypted VPN connection. ▶ Remote access must be via two-factor authentication.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's mobile device policy. We have inspected that VPN connection is encrypted. We have by samples inspected that antivirus and VPN is installed on all devices.	No exceptions noted.

A.6: Organisation of information security and internal organisation		
Control objectives ▶ *To establish a managerial basis to initiate and control the implementation and operation of information security in the organisation.* ▶ To ensure that employees and contractors understand their responsibilities and are suited to the roles for which they are intended.		
Control activity	**Test performed by BDO**	**Result of test**
	We have though samples inspected that two-factor authentication is required when accessing systems and data remotely.	

A.7: Employee safety

Control objectives

- *To ensure that employees and contractors understand their responsibilities and are suited to the roles for which they are intended.*
- *Ensuring employees and contractors are aware of and live up to their information security responsibilities.*
- *To protect the interests of the organisation as part of the change or termination of the employment relationship*

Control activity	Test performed by BDO	Result of test
Screening ▶ The service provider performs screening of potential employees before hiring in the form of interviews and test cases.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for employment and observed that the service provider has a checklist for employment which among other things include obtaining a criminal record. We have by inquiry been informed that no new employees have access to relevant data. Consequently, we have not been able to test for implementation.	We have identified that there have been no cases of employment during the period. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.
Terms and conditions of employment ▶ The contract describes the persons concerned and the organisation's responsibility for information security. ▶ All employees have signed an employment contract containing a provision on professional secrecy. ▶ External suppliers/consultants are subject to a duty of confidentiality when entering into a contract.	We have made inquiries with relevant personnel at the service provider. We have inspected the safety manual and contract of employment. We have by samples inspected that the contract of employment includes a duty of confidentiality. We have by samples observed that employees have approved to have read and understood the service provider's information security policies. We have by inquiry been informed that no external suppliers have been involved in the period.	We have identified that there have been no cases of employment during the period. Therefore, we cannot test the control for implementation and efficiency. We have identified that service provider does not give suppliers access to relevant data. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.

A.7: Employee safety

Control objectives

- *To ensure that employees and contractors understand their responsibilities and are suited to the roles for which they are intended.*
- *Ensuring employees and contractors are aware of and live up to their information security responsibilities.*
- *To protect the interests of the organisation as part of the change or termination of the employment relationship*

Control activity	Test performed by BDO	Result of test
Management responsibilities ▶ Management ensures that all employees and contractors are informed about and maintain the service provider's requirements for information security.	We have made inquiries with relevant personnel at the service provider. We have inspected that employees have been introduced to training in data protection and GDPR. We have observed that employees have approved to have read and understood the service provider's policies. We have observed that the service provider shares information about GDPR and information security regularly.	We have identified that service provider does not give contractors access to relevant data. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.
Awareness of education and training in information security ▶ The service provider holds awareness training of new employees in accordance with data protection and information security, in continuation of the employment. ▶ An introductory course is held for new employees, including information security. ▶ The service provider conducts ongoing awareness training and quizzes of employees in accordance with information security and handling thereof.	We have made inquiries with relevant personnel at the service provider. We have inspected that new employees have a procedure for introduction and training in data protection and GDPR. We have inspected that the service provider has not hired any new employees with access to relevant data. We have observed that employees have approved to have read and understood the service provider's policies. We have observed that the service provider shares information about GDPR and information security regularly. We have inspected that all employees participated in disaster recovery day.	We have identified that there have been no cases of employment during the period. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.

A.7: Employee safety

Control objectives

- *To ensure that employees and contractors understand their responsibilities and are suited to the roles for which they are intended.*
- *Ensuring employees and contractors are aware of and live up to their information security responsibilities.*
- *To protect the interests of the organisation as part of the change or termination of the employment relationship*

Control activity	Test performed by BDO	Result of test
	We have inspected that employees' complete quizzes in information security.	
Sanctions ▶ Rules have been made for sanctions.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's safety manual. We have observed that in case of violation the management will consider sanctions based on the specific case. By inquiry, we have informed that there has been no need for sanctions in the period.	We have identified that there has been no need for sanctions in the period. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.
Termination or change of employment ▶ The service provider has developed and implemented a procedure for offboarding retired employees. ▶ Upon resignation, the employee is informed that the signed confidentiality agreement is still valid.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for employment. We have by samples inspected that the signed confidentiality agreement is still valid after resignation. We have inspected that resigned employees are not presented with rights in the service provider's systems.	No exceptions noted.

A.8: Asset Management

Control objectives

- *To identify the organisation's assets and define appropriate responsibilities for its protection.*
- *To ensure appropriate protection of information that is in proportion to the importance of the information to the organisation.*
- *To prevent unauthorised publication, alteration, removal, or destruction of information stored on media.*

Control activity	Test performed by BDO	Result of test
Ownership of assets ▶ Each asset used is assigned to an owner.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider keeps a list of assets which also includes which employees the assets are assigned to.	No exceptions noted.
Accepted use of assets ▶ The service provider has established rules for accepted use of assets and information.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider has established rules for accepted use of assets and information.	No exceptions noted.
Return of assets ▶ In connection with the termination of employment, handed over assets are returned.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's safety manual and observed that all assets are to be retuned upon termination of employment. We have inspected that no assets are assigned to anyone that are not employed.	No exceptions noted.
Asset management ▶ The service provider has prepared procedures for how assets may be used, e.g., compiled a whitelist of pages employees must access via the Internet.	We have made inquiries with relevant personnel at the service provider.	No exceptions noted.

A.8: Asset Management

Control objectives

- *To identify the organisation's assets and define appropriate responsibilities for its protection.*
- *To ensure appropriate protection of information that is in proportion to the importance of the information to the organisation.*
- *To prevent unauthorised publication, alteration, removal, or destruction of information stored on media.*

Control activity	Test performed by BDO	Result of test
	We have inspected that the service provider has a procedure for how assets may be used, including a whitelist of pages employees can access via the internet.	
Disposal of media - The service provider has developed and implemented a procedure for disposing of media where personal information is stored in a secure manner. - The service provider itself ensures the disposal of media in a responsible manner, including media where personal information is stored, which ensures that stored personal information cannot be accessed.	We have made inquiries with relevant personnel at the service provider. We have inspected disposal, destruction, and reuse policy. We have observed that disposal of media with personal information complies with best practice. By inquiry, we have been informed that no IT equipment was disposed during the period.	We have identified that there has been no disposal of media during the period. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.

A.9: Access Management

Control objectives

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To prevent unauthorised access to systems and applications.*

Control activity	Test performed by BDO	Result of test
Access management policy ▶ Access management procedure is set up to manage registrations and de-registrations of user access.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for access management. We have observed that internal user rights are managed through 1Password.	No exceptions noted.
Access to networks and network services ▶ The service provider gives all employees access to networks and network services that they are authorised to use.	We have made inquiries with relevant personnel at the service provider. We have inspected that all employees have access to the network.	No exceptions noted.
User registration and deregistration ▶ The service provider has set up a procedure for registering and deregistering the user in connection with the allocation of access rights.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for access management. We have inspected that the management approves user access rights. We have inspected that the service provider has removed access rights of former employees.	No exceptions noted.

A.9: Access Management

Control objectives

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To prevent unauthorised access to systems and applications.*

Control activity	Test performed by BDO	Result of test
Allocation of user access ▶ The service provider has established an access control procedure for managing the allocation and revocation of access rights.	We have made inquiries with relevant personnel at the service provider. We have observed that internal user access is managed through 1Password.	No exceptions noted.
Management of privileged access rights ▶ Privileged user rights are assigned based on work-related needs.	We have made inquiries with relevant personnel at the service provider. By inquiry, we have been informed that privileged user rights are assigned through the same procedure as normal user rights. We have inspected that the management approves user access rights.	No exceptions noted.
Review of user access rights ▶ Users and user rights are reviewed every quarter month.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's annual cycle and observed that user rights are reviewed every six months. We have observed that user rights were reviewed twice during the period.	No exceptions noted.
Use of passwords	We have made inquiries with relevant personnel at the service provider.	No exceptions noted.

A.9: Access Management

Control objectives

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To prevent unauthorised access to systems and applications.*

Control activity	Test performed by BDO	Result of test
▶ The service provider has established requirements for passwords which must be followed by all employees and external consultants.	We have inspected that all login is through 1Password. We have by samples inspected that all employees have established two-factor authentication for remote access.	
Limited access to information ▶ The service provider has restricted employees' and customers' access to information, cf. work-related needs and the current contract with the customer, respectively.	We have made inquiries with relevant personnel at the service provider. We have inspected an extract of persons with access to the customers data and observed that only employees with work-related needs can access the customers data.	No exceptions noted.
Procedure for secure log-on ▶ The service provider has established logical access control for systems with personal information, including two-factor authentication.	We have made inquiries with relevant personnel at the service provider. We have inspected that all login is through 1Password. We have by samples inspected that all employees have established two-factor authentication for remote access.	No exceptions noted.
Password management system ▶ The service provider has set up password management systems and these are active.	We have made inquiries with relevant personnel at the service provider. We have inspected that all login is through 1Password. We have observed that there are three administrators who are part of Management or the board of directors.	No exceptions noted.

A.9: Access Management

Control objectives

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To prevent unauthorised access to systems and applications.*

Control activity	Test performed by BDO	Result of test
Use of privileged system programs ▶ Only authorised employees can use system programmes that can bypass system and application controls.	We have made inquiries with relevant personnel at the service provider. We have inspected that all login is through 1Password. We have inspected that there are two administrators in 1Password and observed that these are part of Management.	No exceptions noted.
Access Control to Program Source Code ▶ Access to the Program Source code is limited to relevant users.	We have made inquiries with relevant personnel at the service provider. We have inspected that access to the source code is limited to employees with work-related needs.	No exceptions noted.

A.10: Encryption

Control objectives

- *To ensure the correct and efficient use of cryptography to protect the confidentiality, authenticity and/or integrity of information.*

Control activity	Test performed by BDO	Result of test
Encryption of personal data ▶ The service provider has implemented an encryption policy for encryption of personal data. The policy defines the strength and protocol for encryption. ▶ Portable media with personal data are encrypted. ▶ When transmitting confidential and sensitive personal data via the internet and e-mail encryption is applied.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's encryption policy. We have observed that the service provider uses Permido for safe external communication. We have inspected that SSH jumphost is established.	No exceptions noted.
Administration of keys ▶ Processes and procedures are implemented for creation and maintenance of encryption keys at the customers who have specified the need in their contract with the service provider.	We have made inquiries with relevant personnel at the service provider. We have inspected that processes and procedures are implemented for creation and maintenance of encryption keys at the customers who have specified the need in their contract with service provider.	No exceptions noted.

A.11: Physical protection and environmental protection

Control objectives

- *To ensure that procedures exist for accessing the service provider's sites and that sites are classified.*
- *To ensure a stable supply to the service provider's locations.*
- *To ensure that there is no unauthorised access to the service provider's sites.*

Control activity	Test performed by BDO	Result of test
Physical security ▶ Physical perimeter security has been established to protect areas that contain personal information. The physical perimeter security is in accordance with the adopted safety requirements.	We have made inquiries with relevant personnel at the service provider. We have by inquiries been informed that data is hosted by an external hosting supplier. We have inspected audit reports from the hosting supplier and observed that there are no exceptions noted in relation to the physical security.	No exceptions noted.
Physical access control ▶ Physical access controls have been established, which prevent the likelihood of unauthorised access to the service provider's offices, facilities and personal data, including ensuring that only authorised persons have access. ▶ All accesses are registered and logged. ▶ The physical access to the service providers offices and facilities is reviewed on an ongoing basis and at least once a year.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's overview of keys to the office. We have observed that all accesses are registered and logged. We have observed that access to the office is reviewed on an ongoing basis.	No exceptions noted.
Securing offices, premises and facilities equipment and assets for the organisation ▶ Physical security requirements for offices, premises and facilities have been established.	We have made inquiries with relevant personnel at the service provider. We have by inquiries been informed that data is hosted by an external hosting supplier.	No exceptions noted.

A.11: Physical protection and environmental protection		
Control objectives ▶ *To ensure that procedures exist for accessing the service provider's sites and that sites are classified.* ▶ *To ensure a stable supply to the service provider's locations.* ▶ *To ensure that there is no unauthorised access to the service provider's sites.*		
Control activity	**Test performed by BDO**	**Result of test**
	We have inspected audit reports from the hosting supplier and observed that there are no exceptions noted in relation to the physical security.	
Protection against external and environmental threats ▶ The service provider has established controls for protection against external and environmental threats, including compliance with specified requirements for server rooms including the following conditions.	We have made inquiries with relevant personnel at the service provider. We have by inquiries been informed that data is hosted by an external hosting supplier. We have inspected audit reports from the hosting supplier and observed that there are no exceptions noted in relation to the physical security.	No exceptions noted.
Work in safe areas ▶ The service provider has set up safe areas.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider has set up a safe office.	No exceptions noted.
Location and protection of equipment ▶ The service provider has ensured that equipment is located in safe premises to protect against unauthorised access and environmental threats.	We have made inquiries with relevant personnel at the service provider. We have by inquiries been informed that data is hosted by an external hosting supplier. We have inspected audit reports from the hosting supplier and observed that there are no exceptions noted in relation to the physical security.	No exceptions noted.

A.11: Physical protection and environmental protection

Control objectives

- *To ensure that procedures exist for accessing the service provider's sites and that sites are classified.*
- *To ensure a stable supply to the service provider's locations.*
- *To ensure that there is no unauthorised access to the service provider's sites.*

Control activity	Test performed by BDO	Result of test
Security of supply ▶ Equipment is protected against currents and other disturbances. ▶ Cables which carry data or support telecommunications must be protected.	We have made inquiries with relevant personnel at the service provider. By inquiry, we have been informed that data is hosted by an external hosting supplier. We have inspected audit reports from the hosting supplier and observed that there are no exceptions noted in relation to the physical security.	No exceptions noted.
Equipment maintenance ▶ Equipment is protected against currents and other disturbances. ▶ Cables which carry data or support telecommunications must be protected. ▶ Equipment maintenance follows a maintenance schedule and is performed by authorised personnel.	We have made inquiries with relevant personnel at the service provider. By inquiry, we have been informed that data is hosted by an external hosting supplier. We have inspected audit reports from the hosting supplier and observed that there are no exceptions noted in relation to the physical security.	No exceptions noted.
Securing equipment and assets outside the organization ▶ Equipment outside the organisation must not be left unattended in public places. ▶ Access to the organisation's server from remote workstations can only be accessed via VPN access.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's safety manual and observed that equipment outside the organisation must not be left unattended in public places. We have by samples inspected that all employees have established two-factor authentication for remote access.	No exceptions noted.

A.11: Physical protection and environmental protection

Control objectives

- *To ensure that procedures exist for accessing the service provider's sites and that sites are classified.*
- *To ensure a stable supply to the service provider's locations.*
- *To ensure that there is no unauthorised access to the service provider's sites.*

Control activity	Test performed by BDO	Result of test
Unsupervised user equipment ▶ The service provider has established rules for leaving equipment unattended.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's safety manual and observed that equipment outside the organisation must not be left unattended in public places.	No exceptions noted.
Policies for tidy desk and blank screen ▶ Screen lock is activated automatically after 15 minutes. ▶ Employees must activate screen lock when leaving the client. ▶ Physical material with personal information is stored in a locked cupboard when the material is left. ▶ Physical material may only be printed with the 'follow-me' function and must be removed immediately from the printer.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for clean desk and observed that credential data must not be left available for others. We have observed that screen lock is activated after maximum 15 minutes. We have inspected that automatic screen lock is activated on the employees' computers.	No exceptions noted.

A.12: Operational reliability

Control objectives

- *To ensure proper and safe operation of information processing facilities.*

Control activity	Test performed by BDO	Result of test
Documented operating procedures ▶ Operating procedures have been developed and made available to relevant employees.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's operation and maintenance process. We have inspected that the process is implemented and works effectively.	No exceptions noted.
Change management ▶ The service provider has established change management procedures.	We have made inquiries with relevant personnel at the service provider. We have observed that the service provider practices the security-by-design principles in relation to development and change. We have through samples inspected that the change management procedure has been implemented and works effectively during the period.	No exceptions noted.
Capacity management ▶ Capacity management documentation (production environment monitoring, including uptime, performance, and capacity).	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's production environment monitors. We have inspected documentation for established monitoring system which includes uptime, performance, and capacity. Using a random sample, we have inspected that the system sends notifications on alarms and that the service provider evaluates.	No exceptions noted.

A.12: Operational reliability

Control objectives

- *To ensure proper and safe operation of information processing facilities.*

Control activity	Test performed by BDO	Result of test
Separation of development, testing and production environment ▶ A functional separation between development and operation has been introduced. ▶ Modifications of functionality are tested before it is put into operation. ▶ Development and testing are performed in development environments that are separate from production systems. ▶ A version control system is used which registers all changes in source code. ▶ Development and test environments are separate.	We have made inquiries with relevant personnel at the service provider. We have observed that separation between development and operations has been established. We have observed that all changes in the platform are registered. We have through samples inspected that the change management procedure has been implemented and works effectively during the period.	No exceptions noted.
Malware protection ▶ Controls are implemented for detection, prevention, and recovery to protect against malware, combined with appropriate user awareness.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's safety manual and observed that all computers must have antivirus installed. We have by samples inspected that antivirus is installed.	No exceptions noted.
Data backup and recovery ▶ Systems and data are backed up daily. ▶ Backup storage is outsourced to sub-service provider. ▶ Restore tests are performed once a year.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's security policy and observed that systems and data must be backed up daily and restore tests performed regularly. We have observed that daily, weekly, and monthly backup is implemented.	No exceptions noted.

A.12: Operational reliability		
Control objectives ▶ *To ensure proper and safe operation of information processing facilities.*		
Control activity	**Test performed by BDO**	**Result of test**
	We have observed that monthly backup is stored for three months. We have inspected that the service provider performed restore test in February 2025.	
Event log ▶ All successful and unsuccessful attempts to access the service provider's systems and data are logged. ▶ All user changes in system and databases are logged.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for logging. We have inspected that procedure for logging is implemented and works effectively including that all successful and unsuccessful attempts to access the systems and databases are logged.	No exceptions noted.
Protection of log information ▶ The service provider has restricted who can access log data. ▶ Log data is stored in separate locations that cannot be accessed by one person.	We have made inquiries with relevant personnel at the service provider. We have inspected that the people with access to logging is a limited group. We have observed that log data is stored in three separate locations and cannot be accessed by one person.	No exceptions noted.
Administrator and operator log ▶ The service provider logs administrator and operator activities. ▶ The log is deleted after the stipulated retention period. ▶ The service provider stores logs for 6 months.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for logging.	No exceptions noted.

A.12: Operational reliability		
Control objectives ▶ *To ensure proper and safe operation of information processing facilities.*		
Control activity	**Test performed by BDO**	**Result of test**
	We have inspected that logging is implemented and works effectively including log of administrator and operator activities. We have observed that logs are stored for 6 months.	
Time synchronization ▶ The service provider has enabled time synchronisation.	We have made inquiries with relevant personnel at the service provider. We have observed that time synchronisation is enabled.	No exceptions noted.
Managing technical vulnerabilities ▶ The service provider obtains information about technical vulnerabilities. ▶ The service provider has taken a position on identified vulnerabilities.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider has performed monthly vulnerability scans. We observed a few vulnerabilities has been identified. We have inspected that the service provider TRUST management has reviewed and accepted the vulnerability.	No exceptions noted.
Restrictions on software installation ▶ The service provider has established rules for software installations.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider has an overview of software, services, and settings on employees' computers. We have inspected that the service provider has established rules for what can be downloaded on the employees' computers.	No exceptions noted.

A.12: Operational reliability

Control objectives

- *To ensure proper and safe operation of information processing facilities.*

Control activity	Test performed by BDO	Result of test
Configuration management ▶ The service provider ensures that hardware, software, services, and network functions correctly in relation to security settings, and that these settings are configured so they cannot be changed.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider has an overview of software, services, and settings on employees' computers. We have inspected that the service provider has established rules for what can be downloaded on the employees' computers.	No exceptions noted.
Installation of software on operational systems ▶ The service provider has implemented procedures for software installation. ▶ The service provider has established rules for software installations.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider has an overview of software, services, and settings on employees' computers. We have inspected that the service provider has established rules for what can be downloaded on the employees' computers.	No exceptions noted.

A.13: Communication security

Control objectives

- *To ensure the protection of information in networks and of supporting information processing facilities.*

Control activity	Test performed by BDO	Result of test
Network management ▶ The network topology is structured according to best-practice principles, which means that servers that run applications cannot be accessed directly from the Internet. ▶ The service provider uses known network technologies and mechanisms (Firewall/Intrusion Detection-System/Intrusion Prevention System) to protect internal network.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider's network topology and observed that it complies with best practice standard. We have observed that all access to the service provider's data is through an VPN connection.	No exceptions noted.
Securing network services ▶ The service provider has implemented/required appropriate security measures to protect its network services.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider has implemented appropriate security measures to protect its network services.	No exceptions noted.
Network splitting ▶ The service provider has divided its network so that the systems cannot communicate directly.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider's network topology and observed that it complies with best practice standard. We have observed that all access to the service provider's data is through an VPN connection.	No exceptions noted.
Information transfer agreements ▶ The service provider has entered into information transfer agreements.	We have made inquiries with relevant personnel at the service provider.	We have identified that no request for data has happened in the period. Therefore, we cannot test the control for implementation and efficiency.

A.13: Communication security		
Control objectives ▶ *To ensure the protection of information in networks and of supporting information processing facilities.*		
Control activity	**Test performed by BDO**	**Result of test**
	We have inspected the service provider's procedure for customer termination and observed that data must be deleted or transferred. We have by inquiry been informed that no request for data has happened in the period.	No exceptions noted.
Confidentiality and confidentiality agreements ▶ The service provider has set requirements for confidentiality and confidentiality agreements regarding information transfers.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's safety manual and observed that confidentiality agreement is a part of the employment contract. We have by samples inspected that the employment contract contains a confidentiality agreement.	No exceptions noted.

A.14: Acquisition, development and maintenance of systems		
Control objectives ▶ *To ensure that information security is an integral part of information systems throughout the life cycle. This also includes the requirements for information systems which provide services over public networks.*		
Control activity	**Test performed by BDO**	**Result of test**
Analysis and specification of information security requirements ▶ Information security requirements and requirements for the processing of personal data is included in an early assessment of projects/systems.	We have interviewed relevant personnel with the service provider. We have observed that the service provider works according to privacy-by-design principles in relation to development and changes. We have through samples inspected that relevant development projects are risk assessed.	No exceptions noted.
Secure development policy ▶ The service provider has developed procedures and controls for the development of systems and software in the organisation.	We have interviewed relevant personnel with the service provider. We have observed that the service provider works according to privacy-by-design principles in relation to development and changes. We have through random samples inspected that the development procedures have been implemented and works effectively during the period.	No exceptions noted.
Procedure for managing system changes ▶ The service provider has developed procedures for system changes.	We have interviewed relevant personnel with the service provider. We have observed that the service provider works according to privacy-by-design principles in relation to development and changes. We have through random samples inspected that the change management procedure has been implemented and works effectively during the period.	No exceptions noted.

A.14: Acquisition, development and maintenance of systems		
Control objectives ▶ *To ensure that information security is an integral part of information systems throughout the life cycle. This also includes the requirements for information systems which provide services over public networks.*		
Control activity	**Test performed by BDO**	**Result of test**
Technical review of applications after changes to operating platforms ▶ The service provider conducts appropriate testing of new systems and system changes.	We have interviewed relevant personnel with the service provider. We have observed that the service provider works according to privacy-by-design principles in relation to development and changes. We have through random samples inspected that the change management procedure has been implemented and works effectively during the period.	No exceptions noted.
Principles for the development of secure systems ▶ The service provider follows its established system change and system development procedures.	We have interviewed relevant personnel with the service provider. We have observed that the service provider works according to privacy-by-design principles in relation to development and changes. We have through random samples inspected that the change management and development procedure has been implemented and works effectively during the period.	No exceptions noted.
Securing test data ▶ Anonymised test data is used in the development and test environment.	We have interviewed relevant personnel with the service provider. We have observed that data in the development and test environment is fictional.	No exceptions noted.

A.15: Supplier relations

Control objectives

- *To ensure the protection of the organisation's assets to which suppliers have access.*

Control activity	Test performed by BDO	Result of test
Supplier information security policy ▶ The service provider has established information security requirements for subcontractors used. ▶ The service provider has limited subcontractors' access to the service provider's systems in relation to the subcontractor's work-related needs.	We have interviewed relevant personnel with the service provider. We have inspected the service providers safety manual and observed that the service provider has established a policy for sub-service providers. We have observed that all sub-service providers must be approved by the customers. We have observed that all sub-service providers are approved by the customers. By inquiry, we have been informed that the sub-service providers do not have direct access to the customers data.	We have identified that no new sub service providers have been taken into use during the period. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.
Management of security in Supplier Agreements ▶ Information security requirements have been agreed with relevant subcontractors	We have interviewed relevant personnel with the service provider. We have observed that the service provider has established information security agreements with the sub service providers.	No exceptions noted.
Supply Chain for Information and Communication Technology (ICT) ▶ Information security requirements agreed with subcontractors include requirements for the supply chain for ICT services and products.	We have interviewed relevant personnel with the service provider. We have observed that the service provider has established information security agreements with the sub service providers, including requirements for the supply chain for ICT services and products.	No exceptions noted.

A.15: Supplier relations

Control objectives

- *To ensure the protection of the organisation's assets to which suppliers have access.*

Control activity	Test performed by BDO	Result of test
Monitoring the review of supplier services ▶ The service provider performs inspections, including obtaining and reviewing the sub-service provider's auditor's statements, certifications and the like. ▶ The service provider performs supervision of sub-service providers based on a risk assessment. ▶ The service provider supervises sub-service providers at least once a year, based on a risk assessment.	We have interviewed relevant personnel with the service provider. We have inspected that the service provider has performed inspection and supervision with all sub service providers based on a risk assessment.	No exceptions noted.
Management of changes in supplier services ▶ The service provider decides on any changes to supplier services.	We have interviewed relevant personnel with the service provider. We inspected the service providers safety manual and observed that the service supplier must carry out a due diligence check before new supplier's is put into use, including a review of the audit statement or similar. We have inspected that the service provider has carried out a due diligence check of the new sub-service provider.	We have identified that no new sub service providers have been taken into use during the period. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.
Information security for use of cloud services ▶ The service provider has established risks connected with the use of cloud services. ▶ The service provider has processes for implementing, using, controlling, and cancelling the use of cloud services in accordance with the organisation's information security requirements.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's risk assessment and observed that it involves cloud services. We have by inquiry been informed that the service provider has processes for the use of cloud services. We have been informed that the service provider has not entered new agreements with any cloud services during the period.	We have identified that no new sub service providers have been taken into use during the period. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.

A.16: Management of information security incidents

Control objectives

- *To ensure a uniform and effective method of managing information security incidents, including communication of security incidents and vulnerabilities.*

Control activity	Test performed by BDO	Result of test
Responsibilities and procedures ▶ Management responsibilities and roles have been established in connection with breaches of personal data security. ▶ The service provider has implemented procedure for breach of personal data security.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's procedure for information security breach. We have observed that the service provider has implemented a plan for information security breach. We have inspected that the service providers plan for information security breaches is implemented and works effectively.	We have identified that the service provider has not had any breaches. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.
Reporting of information security incidents ▶ The service provider reports information security incidents to relevant parties.	We have interviewed relevant personnel with the service provider. We have inspected that the service provider communicates incidents to relevant parties.	We have identified that the service provider has not had any breaches. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.
Reporting information security vulnerabilities ▶ The service provider reports information security weaknesses to relevant parties.	We have interviewed relevant personnel with the service provider. We have inspected that the service provider communicates incidents to relevant parties.	We have identified that the service provider has not had any breaches. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.
Assessment and decision on information security incident ▶ The service provider takes a position on any consequences of information security incidents.	We have interviewed relevant personnel with the service provider. We have inspected that the service provider has treated and evaluated incidents.	We have identified that the service provider has not had any breaches. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.

A.16: Management of information security incidents		
Control objectives ▶ *To ensure a uniform and effective method of managing information security incidents, including communication of security incidents and vulnerabilities.*		
Control activity	**Test performed by BDO**	**Result of test**
Dealing with information security incidents ▶ The service provider decides on information security breaches in accordance with the service provider's procedures.	We have interviewed relevant personnel with the service provider. We have inspected that the service provider has treated and evaluated incidents.	We have identified that the service provider has not had any breaches. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.
Experience of information security incidents ▶ The service provider learns from information security incidents.	We have interviewed relevant personnel with the service provider. We have inspected that the service provider reviews and evaluates incidents.	We have identified that the service provider has not had any breaches. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.
Collection of evidence ▶ The service provider collects evidence in the event of information security incidents/weaknesses or incidents.	We have interviewed relevant personnel with the service provider. We have observed that evidence in relation to information security incidents is stored in the ISMS system.	No exceptions noted.

A.17: Information security aspects of emergency, emergency and re-establishment management

Control objectives

- *To ensure a uniform and effective method of managing information security incidents, including communication of security incidents and vulnerabilities.*

Control activity	Test performed by BDO	Result of test
Planning for information security continuity ▶ The service provider has established a contingency plan that ensures rapid response time to restore the availability of and access to personal information in a timely manner in the event of a physical or technical incident.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's contingency plan and observed that the service provider has a procedure for technical or physical incidents.	No exceptions noted.
Implementation of information security continuity ▶ The service provider has implemented controls to ensure the continuity of information security.	We have interviewed relevant personnel with the service provider. We have inspected that the service provider has implemented controls to ensure the continuity of information security. We have inspected that the service provider performs annual restore test and test of the contingency plan.	No exceptions noted.
Verify, review and evaluate information security continuity ▶ The service provider has established periodic testing of the contingency plan in order to ensure that the contingency plans are up-to-date and effective in critical situations. ▶ Contingency tests are documented and evaluated.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's contingency plan and observed that the service provider has a procedure for technical or physical incidents. We have observed that the service provider has tested the contingency plan in August 2024. We have observed that the service provider has documented and evaluated the test.	No exceptions noted.

A.18: Compliance		
Control objectives ▶ *To prevent violation of legal, regulatory, or contractual requirements in relation to information security and other security requirements.*		
Control activity	**Test performed by BDO**	**Result of test**
Identification of applicable legislation and contractual requirements ▶ The service provider has an overview of current legislation and contract requirements. ▶ The service provider regularly checks whether new rules affect the service provider's treatment.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's procedure for identification of requirements. We have observed that the service provider has an overview of external security requirements. We have observed that the overview is updated on an ongoing basis.	No exceptions noted.
Intellectual property rights ▶ The service provider has a procedure for ensuring that applicable legislation and contractual requirements are complied with.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's procedure for identification of requirements. We have observed that the service provider has an overview of external security requirements. We have observed that the service provider reviews that contractual requirements are complied with.	No exceptions noted.
Privacy and protection of personal information ▶ The service provider has ensured that the privacy and rules protection of personal data are complied with in its processing activities.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's data processor agreement and observed that the service provider has guidelines in case of illegal instructions. We have observed that the service provider's guidelines are reviewed in October 2024.	No exceptions noted.

A.18: Compliance		
Control objectives ▶ *To prevent violation of legal, regulatory, or contractual requirements in relation to information security and other security requirements.*		
Control activity	**Test performed by BDO**	**Result of test**
	We have inspected that the service provider evaluates rules are complied with on a monthly basis.	
Regulation of cryptography ▶ Cryptographic rules are complied with during the service provider's processing.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's encryption policy. We have observed that the service provider uses Permido for safe external communication. We have inspected that SSH jumphost is established.	No exceptions noted.
Independent review of information security ▶ The service provider performs regular reviews of their policies.	We have interviewed relevant personnel with the service provider. We have inspected the annual cycle and observed that the service provider's policies are reviewed annually. We have observed that policies are reviewed.	No exceptions noted.
Compliance with safety policies and safety standards ▶ The service provider carries out regular reviews of relevant procedures and controls.	We have interviewed relevant personnel with the service provider. We have inspected the annual cycle and observed that the service provider's procedures and controls are reviewed annually. We have observed that procedures and controls are reviewed.	No exceptions noted.
Examination of technical conformity ▶ The service provider conducts a regular review of compliance with the organisation's information security policies and standards.	We have interviewed relevant personnel with the service provider.	No exceptions noted.

A.18: Compliance		
Control objectives ▶ *To prevent violation of legal, regulatory, or contractual requirements in relation to information security and other security requirements.*		
Control activity	**Test performed by BDO**	**Result of test**
	We have inspected the annual cycle and observed that the service provider's procedures and policies are reviewed annually. We have observed that the service provider has tested the contingency plan in August 2024. We have observed that the service provider has documented and evaluated the test.	

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

CVR-NR. 20 22 26 70

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Allan Juhl
CEO
Serienummer: f05ee19d-619d-4f3a-8665-0620bfc4b2e9
IP: 80.209.xxx.xxx
2025-05-01 10:34:55 UTC

Nicolai Tobias Visti Pedersen
Statsautoriseret revisor
Serienummer: 096fe1fc-de80-4d55-8c69-fc2fb761227d
IP: 62.66.xxx.xxx
2025-05-01 10:42:57 UTC

Mikkel Jon Larssen
BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670
Partner
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 77.243.xxx.xxx
2025-05-01 11:54:05 UTC