

CONTENTS

1. INDEPENDENT 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
Risk Assessment.....	10
Technical and Organisational Security Measures and Other Controls	10
Changes during the period from 1 April 2024 to 31 March 2025	14
Complementary controls with the Controller	14
4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND THE RESULT OF TESTS	15
Control area A	17
Control area B.....	19
Control area C	28
Control area D	34
Control area E.....	35
Control area F.....	36
Control area H	38
Control area I.....	39

1. INDEPENDENT AUDITOR'S REPORT

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD 1 APRIL 2024 TO 31 MARCH 2025 ON THE DESCRIPTION OF THE EMENTO PRODUCT SUITE AND NAME OF THE COMPANY AND RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH ACT ON SUPPLEMENTARY PROVISIONS

To: The Management of Emento A/S
Emento A/S' Customers

Scope

We have been engaged to report on Emento A/S' (the Data Processor) description in section 3 of the Emento Product Suite and the related technical and organisational measures and other controls, relating to processing and protection of personal data in accordance with the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions to the Regulation (Danish Data Protection Act), and on the design and operating effectiveness of the technical and organisational measures and other controls related to the control objectives stated in the description for the period 1 April 2024 to 31 March 2025.

The Data Processor's Responsibilities

The Data Processor is responsible for preparing the statement in section 2 and the accompanying description including the completeness, accuracy, and method of presenting the statement and the description. Furthermore, the Data Processor is responsible for providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Auditor's Independence and Quality Control

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 to express an opinion on the Data Processor's description in section 3 and on the design and operating effectiveness of the controls related to the control objectives stated in the description, based on our procedures.

We conducted our engagement in accordance with the International Standard on Assurance Engagements 3000, "Reports Other Than Audits or Reviews of Historical Financial Information". That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are appropriately designed.

An assurance engagement to report on the description, design and operating effectiveness of controls at a Data Processor involves performing procedures to obtain evidence about the disclosures in the Data Processor's description and about the design and operating effectiveness of the controls. The procedures selected

depend on the auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that controls are not appropriately designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the appropriateness of the objectives stated therein, and the suitability of the criteria specified by the Data Processor and described 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 Data Processor

The Data Processor's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the use of the Emento product suite and Emento A/S, that each individual Controller may consider important in their own environment. Also, because of their nature, controls at a Data Processor may not prevent or detect all breaches of the personal data security. Furthermore, the projection of any evaluation of the operating effectiveness of controls to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

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

- a. The description presents fairly the Emento Product Suite and the related technical and organisational measures and other controls, relating to processing and protection of personal data in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act, as designed and implemented for the period 1 April 2024 to 31 March 2025.
- b. The technical and organisational measures and other controls, relating to the control objectives stated in the description were appropriately designed for the period 1 April 2024 to 31 March 2025.
- c. The technical and organisational measures and other 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 Test of Controls

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

Intended Users and Purpose

This report is intended solely for data controllers who have used the Emento Product Suite, and who have a sufficient understanding to consider it along with other information, including information about the technical and organisational measures and other controls operated by the data controllers themselves when assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

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 processes personal data in relation to the Emento Product Suite to our customers, who are Data Controllers according to the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions (the Danish Data Protection Act).

The description has been prepared for Data Controllers who have used the Emento Product Suite and who have a sufficient understanding to consider the description along with other information, including information about the technical and organisational measures and other controls operated by the data controllers themselves in assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

Emento A/S uses sub-processors. The relevant control objectives and related technical and organisational measures and other controls of these sub-processors are not included in the accompanying description.

Emento A/S confirms that the accompanying description in section 3 fairly presents the Emento product suite and the related technical and organisational measures and other controls for the period 1 April 2024 to 31 March 2025. The criteria used in making this statement were that the accompanying description:

1. Presents the Emento Product Suite, and how the related technical and organisational measures and other controls were designed and implemented, including:
 - The types of services provided, including the type of personal data processed.
 - The processes in both IT systems and business procedures applied to process personal data and, if necessary, correct and delete personal data as well as limiting the processing of personal data.
 - The procedures used to ensure that data processing has taken place in accordance with contract, instructions, or agreement with the data controller.
 - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality.
 - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation.
 - The procedures supporting in the event of breach of personal data security that the data controller may report this to the supervisory authority and inform the data subjects.
 - The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed.
 - The controls that we, with reference to the delimitation of the Emento Product Suite would have been designed and implemented by the data controllers, and which, if necessary to achieve the control objectives, are identified in the description.
 - The other aspects of the control environment, risk assessment process, information systems and communication, control activities and monitoring controls that are relevant to the processing of personal data.
2. Includes relevant information on changes in the Emento Product Suite and the related technical and organisational measures and other controls throughout the period.

3. Does not omit or distort information relevant to the scope of the Emento Product Suite and the related technical and organisational measures and other controls described while acknowledging that this description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the Emento Product Suite that the individual data controllers might consider important in their environment.

Emento A/S confirms that the technical and organisational measures and other controls related to the control objectives stated in the accompanying description were suitable designed for the period 1 April 2024 to 31 March 2025. The criteria we used in making this statement were that:

1. The risks threatening achievement of the described control objectives 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 applied consistently as designed, including manual controls were performed by persons with appropriate competencies and rights, in the entire period from 1 April 2024 to 31 March 2025.

Emento A/S confirms that appropriate technical and organisational measures and other controls were implemented and maintained to comply with the agreements with data controllers, good practices for the data processing of data and relevant requirements for Data Processors in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act.

Aarhus, 1 May 2025

Emento A/S

Allan Juhl
CEO

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

GENERAL DESCRIPTION OF EMENTO A/S

Emento A/S is a Danish-owned company developing, operating, maintaining and supporting the Emento Product Suite.

The platform consists of an app aimed at the citizen/patient and a web access aimed at the staff. The staff defines 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.

Emento A/S has approx. 26 employees who are specialised within system development, support, delivery, marketing, sales, finance, GDPR and information security. They are organised in a development and operations department, quality and support department, a delivery department and an administration department.

The administration department controls Emento's security of personal data in relation to the processing that Emento handles on behalf of their clients, including entering into processor agreements, replying to inquiries from the data controller, communication of personal data breach, compliance with internal policies and procedures, etc.

Emento uses DPO Denmark as advisors on GDPR-related questions in DK.

EMENTO PRODUCT SUITE AND PROCESSING OF PERSONAL DATA

Emento provides the Emento Product Suite as a Software-as-a-Service (SaaS) solution in accordance with concluded agreement with public authorities and private companies.

The Emento Product Suite is developed in Denmark and data are hosted within team blues and Hetzners hosting centres, which are located in Skanderborg, Denmark and Nuremberg/Falkenstein, Germany. A data processor agreement has been made between Emento and the hosting providers. Hosting providers may use sub data processors for housing of data and destruction. The hosting providers are responsible for performing the control of these.

Emento processes personal data on behalf of their clients, who are Data Controllers when they apply Emento Product Suite. Emento has entered into data processing agreements with the Controllers on this processing.

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.

The personal data being processed fall within article 6 of the General Data Protection Regulation on ordinary personal data and includes full name, e-mail, profile image, telephone number, and identification, as well as in a few cases, confidential information, such as personal identification number included in article 11 (2) and information about the type of course that the civilian may have as included in article 9 of the General Data Protection Regulation.

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. This solution only contains phone number and in some cases profile image.

MANAGEMENT OF THE SECURITY OF PERSONAL DATA

Emento has prepared requirements for establishing, implementing, maintaining, and improving a management system for the security of personal data, which ensure compliance with the concluded agreements with the Controllers, good data processor practice, and relevant requirements for Data Processors in accordance with the General Data Protection Regulation and the Data Protection Act.

The technical and organisational security measures and other controls for protection of personal data are designed in accordance with the risk assessments and implemented to ensure confidentiality, integrity, and accessibility together with compliance with current data protection legislation. Security measures and controls are wherever possible automated and technically supported by IT systems.

Management of the security of personal data and the technical and organisation security measures and other controls are structured in the following key areas, for which control objectives and control activities have been defined:

THE DATA PROCESSING AGREEMENT	CONTROL AREA	ARTICLE
<p><i>Control area A</i></p> <p>Procedures and controls are complied with to ensure that instructions regarding the processing of personal data are complied with in accordance with the incoming data processing agreement.</p>	<ul style="list-style-type: none"> • Entering into a data processing agreement with the Controller • Instruction for processing of personal data • Compliance with instruction for processing of personal data • Communication of unlawful instruction to the controller 	<ul style="list-style-type: none"> • Art. 28 (3) • Art. 28 (3)(a) • Art. 29 • Art. 32 (4) • Art. 28 (10) • Art. 28 (3)(h)
<p><i>Control area B</i></p> <p>Procedures and controls are followed, which ensure that the data processor has implemented technical measures to ensure relevant processing security.</p>	<ul style="list-style-type: none"> • Risk assessment • Contingency plans in case of physical or technical incidents • Physical access control • Logical access control • Remote workplaces and remote access to systems and data • External communication connections • Encryption of personal data • Firewall • Network security • Anti-virus program • Vulnerability scanning and penetration testing • Back-up and re-establishment of data • Maintenance of system software • Logging in systems, databases, and network, including logging of application of personal data • Monitoring • Repair and service as well as disposal of IT equipment • Testing, assessment and evaluation of the efficiency of the technical and organisational security measures • Development and sustainability of systems • Information security in development and changes • Segregation of development, test and production environments 	<ul style="list-style-type: none"> • Art. 28 (3)(c) • Art. 25

THE DATA PROCESSING AGREEMENT	CONTROL AREA	ARTICLE
	<ul style="list-style-type: none"> Personal data in development and test environments Support assignments 	
<p><i>Control area C</i> Procedures and controls are followed, which ensure that the data processor has implemented organisational measures to ensure relevant processing security.</p>	<ul style="list-style-type: none"> Information Security Policy Review of the information security policy Organisation of information security policy Recruitment of employees Resignation of employees Training and instruction of employees processing personal data Awareness and information campaigns for employees Confidentiality and secrecy agreement with employees Obligations of security of processing and impact assessments Audit and inspection Records of processing activities Storage of the record The Danish Data Protection Agency's access to the record Selection of Data Protection Officer The position of the Data Protection Officer. Tasks of the Data Protection Officer 	<ul style="list-style-type: none"> Art. 28(1) Art. 28 (3)(b) Art. 28 (3)(f) Art. 28 (3)(h) Art. 30 (2), (3) and (4) Art. 33 (2) and (5) Art. 38 Art. 39
<p><i>Control area D</i> Procedures and controls are followed, which ensure that personal data can be deleted or returned if an agreement is entered into with the data controller.</p>	<ul style="list-style-type: none"> Deletion of personal information Return of personal information 	<ul style="list-style-type: none"> Art. 28 (3)(g)
<p><i>Control area E</i> Procedures and controls are followed, which ensure that the data processor only stores personal data in accordance with the agreement with the data controller.</p>	<ul style="list-style-type: none"> Storage of personal data Handling of input and output data materials 	<ul style="list-style-type: none"> Art. 28 (3)(c)
<p><i>Control objectives F</i> Procedures and controls are followed, which ensure that only approved sub-data processors are used, and that the data processor, by following up on their technical and organisational measures to protect the data subjects' rights and the processing of personal data, ensures satisfactory processing security.</p>	<ul style="list-style-type: none"> Sub data processor agreement and instruction Approval of sub data processors Changes to approved sub data processors Overview of approved sub data processors Supervision of sub data processors 	<ul style="list-style-type: none"> Art. 28 (2) and (4)
<p><i>Control area H</i> Procedures and controls are followed, which ensure that the data processor can assist the data controller with the provision, correction, deletion or restriction of information on the processing of personal data to the data subject.</p>	<ul style="list-style-type: none"> The data subject's rights 	<ul style="list-style-type: none"> Art. 28 (3)(e)
<p><i>Control area I</i> Procedures and controls are followed to ensure that any security breaches can be handled in accordance with the data processor agreement entered into.</p>	<ul style="list-style-type: none"> Communication of personal data breach Identification of personal data breaches Registration of personal data breaches Assisting the data controller with handling personal data breaches 	<ul style="list-style-type: none"> Art. 33 (2) Art. 28 (3)(f)

RISK ASSESSMENT

It is Management's responsibility to take initiatives to address the threat scenario that Emento is facing at all times, so that the security measures and controls introduced are appropriate, and the risk personal data breach, is reduced to a proper level.

The appropriate level of security is assessed on a current basis. The assessment takes into consideration risks relating to the accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.

An annual risk assessment is performed as the basis of updating of the technical and organisational security measures and other controls. The risk assessment illustrates the probability and consequences of incidents that may threaten the security of personal data and thereby natural persons' rights and freedoms, including incidental, intentional, and unintentional events. The risk assessment considers the actual technical level and implementation costs.

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES AND OTHER CONTROLS

The technical and organisational security measures and other controls concern all processes and systems, which process personal data on behalf of the Controller. The control objectives and control activities stated in the control schedule are an integral part of the subsequent description.

The Data Processor's guarantees

Emento has introduced policies and procedures ensuring that Emento can provide the sufficient guarantees for completing appropriate technical and organisational security measures in such a way that the processing complies with the requirements of the General Data Protection Regulation and ensures protection of the data subject's rights. Emento has established an organisation of the security of personal data as well as prepared and implemented an information security policy approved by Management, which is reviewed and updated on an ongoing basis. Procedures for recruiting and resignation of employees as well as guidelines for training and instruction of employees processing personal data, including completion of awareness and information campaigns, exist.

Data processing agreement

Emento has introduced policies and procedures for entering into data processing agreements, which ensure that Emento in relation to the client contract enters into a data processing agreement, which states the terms for processing of personal data on behalf of the Controller. Emento applies a template for data processing agreements in accordance with the services to be provided, including information on the use of subprocessors. The data processing agreements are digitally signed and stored electronically.

Instruction for processing of personal data

Emento has introduced policies and procedures ensuring that Emento acts according to the instruction given by the Controller in the data processing agreement. The instruction is maintained with procedures instructing employees in how processing of personal data must be done. Moreover, the procedures ensures that Emento informs the Controller, when their instructions are not perceived to be following data protection legislation.

Subprocessors

Emento has introduced policies and procedures which ensure that subprocessors are assigned the same data protection obligations as stated in the data processing agreement between the Controller and Emento and that the subprocessor may give sufficient guarantees to protection of personal data. Procedures ensure that the Controller gives a preceding specific or general written approval of sub processors, including changes of approved sub processors are controlled.

Emento assesses the sub processor and their guarantees, before an agreement is entered into, to ensure that the subprocessor will be able to comply with the obligations assigned to Emento. Emento monitors their subprocessor on an annual basis based on a risk assessment of the specific processing of personal data by obtaining auditor reports of the type ISAE 3000 or SOC 2, or similar documentation.

Confidentiality and professional secrecy

Emento has introduced policies and procedures ensuring confidentiality at the processing of personal data. All employees at Emento have committed to confidentiality by signing an employment contract containing terms of secrecy and confidentiality.

Technical and organisational security measures

Risk assessment

Emento has completed the technical and organisational security measures on the basis of a risk assessment in connection to confidentiality, integrity and availability. Please refer to separate section about this.

Contingency plans

Emento has established contingency plans, thus, Emento can re-establish the availability of and access to personal data in due time in case of physical and technical events. Emento has established emergency preparedness, which takes effect in these cases. Organisation of an emergency preparedness group is established and guidelines for activation of the emergency preparedness has been introduced.

Emento has designed detailed contingency plans and plans for re-establishment of systems and data, which among other things ensure person independence in connection with activation of the emergency preparedness and the re-establishment. A copy of the plans is stored securely outside Emento's IT systems. The plans are tested and revised on a current basis in connection with changes to systems, etc.

Storage of personal data

Emento has introduced procedures ensuring that personal data are solely stored in accordance with the contract with the Controller and the list of locations in the accompanying data processing agreement.

Physical access control

Emento has introduced procedures ensuring that rooms are protected against unauthorised access. Only persons with a work-related or other legitimate need have access to the rooms, and special security measures have been taken for areas, where personal data is processed. Clients, suppliers, and other visitors must be escorted.

Physical security

Emento has introduced procedures to ensure that servers are protected from unauthorized access, damage, outages, and similar incidents by special security measures. Servers are thus stored in a specially designed server room with physical and electronic access control and logging of accesses. The server room is protected against environmental threats such as fire, water intrusion, moisture, overheating, power failure and over-voltage. Systems for environmental protection of operating facilities are serviced and maintained on an ongoing basis in accordance with the regulations of the respective suppliers. The operating environment is monitored.

Logical access security

Emento has introduced procedures ensuring that access to systems and data are protected by an authorisation system. User is set up with unique user identification and password, and user identification is used in connection with allocation of resources and systems. All allocation of rights in systems is based on a work-related need. An assessment of the users' continued work-related need for access is reviewed at least once annually, including relevancy and correctness of allocated user rights. Procedures and controls support the process of creating, changing, and terminating users and allocated rights as well as review hereof.

The design of rules for i.a. length, complexity, regular changes to and history of password and termination of user account after unsuccessful log-on attempts follows best practice for a secure logical access control. Technical measures have been established to support these rules.

To access guides in the Emento Product Suite app, the user has to be validated with MitID. To access guides in the _Guide app, the user can access with a phone number and a password.

Remote workplaces and remote access to systems and data

Emento has introduced procedures ensuring that access from workplaces outside Emento's premises and remote access to systems and data take place through VPN connections.

External communication connections

Emento has introduced procedures to ensure that external communications connections are secured with strong encryption and that e-mail and other communications containing sensitive personal information are encrypted in the transmission using TLS.

Encryption of personal data

Emento has introduced procedures ensuring that databases containing personal data are encrypted and that the same apply for back-up copies. Recovery keys and certificates are securely stored.

Emento has introduced procedures ensuring that data on personal units, which are not protected by special security measures, is encrypted when put into use, so that access to data is only possible for authorised users. Recovery keys and certificates are stored properly.

Algorithms and levels of encryption used for encryption of units, servers, and data are risk-assessed on a current basis according to the current threat level.

Firewall

Emento has introduced procedures ensuring that traffic between the internet and the network is controlled by a firewall. External access by means of ports in the firewall is limited wherever possible, and access rights are allocated through actual ports for specific segments. Workstations uses firewall.

Network security

Emento has introduced procedures ensuring that networks in relation to use and security are divided into several virtual networks (VLAN), in which traffic between the individual virtual networks are controlled by firewalls. Servers with incorporated firewalls use this to ensure that access is only given to necessary services.

Anti-virus programme

Emento has introduced procedures ensuring that units with access to networks and applications are protected against virus and malware. Antivirus programmes and other protective systems are continually updated and adjusted in relation to the actual threat level, and an ongoing monitoring of these systems has been set up, including periodical testing for functionality.

Vulnerability scanning

Emento has introduced procedures ensuring that a periodic port scanning for the purpose of identifying and prevent technical vulnerabilities in the infrastructure, thus, losses of confidentiality, integrity, and accessibility of systems and data are avoided.

Back-up and re-establishment of data

Emento has introduced procedures ensuring that systems and data are backed up to prevent loss of data or loss of accessibility in the event of critical failures. Back-ups are stored at an alternative location. Back-ups are protected with both physical and logical security measures, which prevent data from falling into the hands of unauthorised persons or that back-ups are destroyed by fire, water, malicious damage, or accidental damage.

Maintenance of system software

Emento has introduced procedures ensuring that system software is updated regularly according to the suppliers' directions and recommendations. Procedures for Patch Management include operating systems, critical services and software installed on servers and workstations.

Logging in systems, databases, and network

Emento has introduced procedures ensuring that logging is set up in accordance with legislative requirements and business needs, based on a risk assessment of systems. The scope and quality of log data are sufficient to identify and demonstrate possible unauthorised use of systems or data, and log data is examined on a current basis for applicability and abnormal conduct. Log data is secured against loss and erasure.

Monitoring

Emento have introduced procedures ensuring that continuing monitoring of systems and technical security measures introduced.

Testing, assessment and evaluation

Emento has introduced procedures for regular testing, assessment and evaluation of the efficiency of the technical and organisational security measures for ensuring the processing security.

Data protection by design and by default

Emento has introduced policies and procedures for developing and maintaining the Emento Product Suite, which ensure a controlled change of process. A change management system for controlling development and change tasks is applied, and every task follows a uniform process initiated by a risk assessment in accordance with the requirements of data protection by design and by default.

Development, testing, and production environments are separate, and segregation of duties is established between employees in the development department and the operation and support department. Each development and change task passes through a testing cycle and anonymised production data are applied as test data. Procedures are introduced for version control, logging and back-up, thus, it is possible to reinstall previous versions.

Deletion and return of personal data

Emento has introduced policies and procedures ensuring that personal data are deleted or returned in accordance with instruction from the Controller, when the processing of personal data terminates at the end of contract with the Controller.

Assistance to the Controller

Emento has introduced policies and procedures ensuring that Emento can assist the Controller in complying with their obligation to reply to requests on executing the data subjects' rights.

Emento has introduced policies and procedures ensuring that Emento can assist the Controller in ensuring compliance with the obligations of article 32 on security of processing, article 33 on notification and communication of personal data breach, and article 34 - 36 on data protection impact assessment.

Emento has introduced policies and procedures ensuring that Emento can provide to the Controller all information necessary to demonstrate compliance with the requirements of the Data Processors. Besides, Emento allows and assists in audits, including inspections performed by the Controller or others, who are authorised to do this by the Controller.

Records of processing activities

Emento has introduced policies and procedures ensuring that a record is kept of categories of processing activities performed on behalf of the Controller. The record is updated regularly and controlled during the annual review of policies and procedures, etc. The record is stored electronically and can be provided for the supervisory authority, by request.

Communication of personal data breach

Emento has introduced policies and procedures ensuring that personal data breaches are registered with detailed information about the event and that the Controller communicates without undue delay after Emento becomes aware of the personal data breach. The registered information makes the Controller able to assess whether the personal data breach must be reported to the supervisory authority and whether the data subjects should be notified.

Data Protection Officer

Emento has introduced procedures to ensure that external communications connections are secured with strong encryption and that email and other communications containing sensitive personal information are encrypted in the shipment using TLS. Emento has appointed a Data Protection Officer, as Emento processes sensitive personal data to a large extent as part of its core business. Emento has also established a Data Protection Officer team and prepared a mandate for it. The Data Protection Officer refers to the Senior Management of Emento, who has prepared a job and job description for the Data Protection Officer, including the tasks of the Data Protection Officer.

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

Emento A/S has not made significant changes of 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 CONTROLLER

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

- The Controller is responsible for ensuring that the administrators' use of the Emento platform and the processing of personal data conducted in the system are in accordance with the data protection legislation.
- The Controller controls the user privileges in the Emento platform, including who are allocated administrator access and which rights the individual administrators are allocated.
- The data controller is responsible for ensuring that the administrators' use of the Emento platform and the processing of personal data carried out in the system take place in accordance with data protection legislation.

4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND THE RESULT OF TESTS

We conducted our engagement in accordance with ISAE 3000, Assurance Reports Other Than Audits or Reviews of Historical Financial Information.

BDO has inspected procedures to obtain evidence of the information in Emento A/S' description of the Emento Product Suite, the design and operating effectiveness of the relating technical and organisational measures and other controls. The procedures selected depend on BDO's assessment, including the assessment of the risks that the description is not fairly presented and that the controls are not appropriately designed or operating effectively.

BDO's test of the design and the operating effectiveness of the relating technical and organisational measures and other controls and their implementation has included the control objectives and related the control objectives and related control activities selected by Emento A/S, and which are described in the check form below.

In the test form, BDO has described the tests carried out which were assessed necessary to obtain reasonable assurance that the stated control objectives were achieved, and that related controls were appropriately designed and operated effectively for the period 1 April 2024 to 31 March 2025.

Test procedures

Test of the design of the relating technical and organisational measures and other controls and their implementation was performed by inquiries, inspection, observation and re-performance.

Type	Description
Inquiry	Inquiries of relevant personnel 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 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 2023 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.

These sub-processors and service organisations' relevant control objectives and related controls are not included in Emento's description of the Emento Product Suite and relevant controls related to operation of the Emento Product Suite. Thus, we have solely assessed the reports and tested the controls at Emento A/S, which ensures appropriate supervision of the sub-processor's compliance with the data processing agreement made between the sub-processor and the data processor and compliance with the General Data Protection Regulation and the Danish Data Protection Act.

Result of test

The result of the test made of technical and organisational measures and other controls has resulted in the following exceptions noted.

An exception exists when:

- Technical and organisational measures and other controls have not been designed or implemented to fulfil a control objective, and
- 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.

Control area A		
Control Objective ► Procedures and controls are followed to ensure that instructions regarding the processing of personal data are complied with in accordance with the data processing agreement entered.		
Control activities	Test performed by BDO	Result of test
Entering a data processing agreement with the Controller <ul style="list-style-type: none"> ► The Data Processor has procedures for entering into written data processing agreements which are in accordance with the services provided by the Data Processor. ► The Data Processor applies a data processing agreement template for entering into data processor agreements. ► When entering a written data processing agreement based on the data controllers' template, the data processor uses a checklist to ensure that it can comply with the data processing agreement. ► Data processing agreements are signed and stored electronically. ► Data processing agreements contain information about the use of sub processors. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected the data processor's procedures for entering new data processing agreements.</p> <p>We have observed that the data processor applies its own or the customer's template for data processing agreements.</p> <p>Using random samples of the data processor's data processing agreements we have observed that the agreements contain information about the use of sub processors.</p> <p>Using random samples of the data processor's data processing agreements we have observed that the agreements are stored electronically and signed.</p>	No exceptions noted.
Instruction for processing of personal data <ul style="list-style-type: none"> ► Data processing agreement contains instructions from data controller(s). ► The Data Processor obtains instruction for processing personal data from the Controller, in connection with entering into a data processor agreement. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected samples of data processing agreements and observed that the data processing agreement contains a general instruction in relation to operation and maintenance of the data controller's service with the data controller.</p>	No exceptions noted.
Compliance with instruction for processing of personal data <ul style="list-style-type: none"> ► The Data Processor solely processes personal data as per instruction from the Controller. ► The Data Processor has created and implemented written procedures regarding processing personal data to ensure that data is only processed based on instructions from data controllers. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected the data processor's template for data processing agreements.</p>	No exceptions noted.

Control area A		
Control Objective ► Procedures and controls are followed to ensure that instructions regarding the processing of personal data are complied with in accordance with the data processing agreement entered.		
Control activities	Test performed by BDO	Result of test
<ul style="list-style-type: none"> ► The Data Processor procedures are looked over and updated regularly and at least annually. ► The Data Processor verifies that it complies with instructions in active data processing agreements. 	<p>We have observed that the data processor solely processes data per instruction from the controller.</p> <p>We have observed that the data processor has implemented procedures regarding illegal instructions.</p> <p>We have observed that the data processor procedures are updated in October 2024.</p> <p>We have inspected that the data processor conducts monthly TRUST meetings in which compliance with instructions are verified.</p>	
Communication of unlawful instruction to the Controller <ul style="list-style-type: none"> ► The Data Processor has prepared a procedure for communication to the Controller when the Controller's instruction is in contravention of the data protection legislation. ► The Data Processor communicates immediately to the Controller, if the Controller's instruction is in contravention of the data protection legislation. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected the data processor's procedure for illegal instructions and observed that the data processor communicates immediately to the controller if the controller's instruction is in contravention of the data protection legislation.</p> <p>We have by request been informed that no incidents have occurred in the period.</p>	<p>We have identified that there have been no incidents with instructions in conflict with the law from the controller. Therefore, we cannot test the control for implementation and efficiency.</p> <p>No exceptions noted.</p>

Control area B		
Control Objective ► Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.		
Control activities	Test performed by BDO	Result of test
Risk Assessment <ul style="list-style-type: none"> ► On an ongoing basis, risk assessment of potential risks for the accessibility, confidentiality and integrity of data is performed, in relation to the data subjects' rights and freedoms. ► The vulnerability of systems and processes is assessed based on identified threats. ► Risks are minimised based on the assessment of their likelihood and consequence. ► Risk assessments are updated on an ongoing basis when needed, but at least once a year. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected the data processor's risk assessment and observed that the risk assessment includes the potential risks for the accessibility, confidentiality, and integrity of data in relation to the data subjects' rights and freedoms.</p> <p>We have observed that the data processor concerns potential risks by implementing preventive actions.</p> <p>We have observed that risks are based on estimated likelihood and consequence.</p> <p>We have observed that the risk assessment is updated and approved by management in June 2024.</p>	No exceptions noted.
Contingency plans in case of physical or technical incidents <ul style="list-style-type: none"> ► The Data Processor has established a contingency plan, which ensures quick response time to restore the accessibility of and access to personal data in a timely manner, in case of a physical or technical incident. ► The Data Processor has established periodic testing of the contingency plan with a view to ensure that the contingency plans are up-to-date and efficient in critical situations. ► Tests of the contingency plans are documented and evaluated. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected the data processor's contingency plan.</p> <p>We have observed that the contingency plan contains a procedure for actions in case of technical or physical incidents.</p> <p>We have inspected the data processor's test of the contingency plan in October 2024 and observed that the test is documented.</p> <p>We have inspected that the data processor has evaluated the test of the contingency plan.</p>	No exceptions noted.
Physical access control	<p>We have made inquiries to relevant staff at the data processor.</p>	No exceptions noted.

Control area B		
Control Objective ► Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.		
Control activities	Test performed by BDO	Result of test
<ul style="list-style-type: none"> ► Physical access control is established, which reduced the possibility for unauthorised access to the Data Processor's offices, facilities and personal data. Only authorised personnel have access. ► All access is registered and logged. ► A regular and annual control of the physical access security measures is performed. 	<p>We have inspected the data processor's overview of keys to the office and observed that key only is delivered to authorised personnel.</p> <p>We have inspected that all access to the office is registered and logged.</p> <p>We have inspected that the data processor performs a regular control of the employees' physical access.</p>	
Logical access control <ul style="list-style-type: none"> ► The Data Processor has implemented procedures for user administration which ensures that user creation and deletion follows a uniformed process and that all user creations are authorised. ► User rights are assigned based on work-related needs. ► Privileged user rights are assigned based on work-related needs. ► Users and user rights are reviewed two times annually. ► All access to systems and data is logged. ► The data processor has established logical access control for systems with personal information, including two-factor authentication. ► The data processor has established rules for password requirements, which must be followed by all employees as well as external consultants. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected the data processor's procedure for employment and observed that user and privileged rights are based on work-related-needs.</p> <p>We have inspected that the data processor reviews users and rights two times annually.</p> <p>We have inspected that the data processor has established two-factor authentication.</p> <p>We have by request been informed that no external consultants have been granted access to the controller's data.</p> <p>We have inspected that all access to systems and data is logged.</p> <p>We have inspected the data processor's password policy based on best practice standards and is implemented through the central setup.</p>	<p>We have identified that the processor does not give contractors access to personal data. Therefore, we cannot test the control for implementation and efficiency.</p> <p>No exceptions noted.</p>
Remote workplaces and remote access to systems and data <ul style="list-style-type: none"> ► All mobile units which have access to personal data must have anti-virus installed and updated. 	<p>We have made inquiries to relevant staff at the data processor.</p>	<p>No exceptions noted.</p>

Control area B		
Control Objective ► Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.		
Control activities	Test performed by BDO	Result of test
<ul style="list-style-type: none"> ► Remote access to the Data Processor's systems and data is via an encrypted VPN connection. ► Remote access must go through two-factor authentication. 	<p>We have inspected the data processor's IT-security policy and observed that all mobile units which have access to personal data must have anti-virus installed and updated.</p> <p>We have through samples observed that all computers have updated antivirus and VPN installed.</p> <p>We have inspected that remote access to the Data Processor's systems and data is via an encrypted VPN connection.</p> <p>We have by samples inspected that the data processor has established two-factor authentication for remote access.</p>	
External communication connections <ul style="list-style-type: none"> ► External access to systems and databases, which are used to process personal data, is done through firewall and VPN. ► Exchange of personal data through e-mail is done by secure e-mail (SikkerMail). ► External communication connections are encrypted. ► The Data Processor has an overview of which external communication connections are approved to access their network. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected that external access to systems and databases is through firewall and VPN.</p> <p>We have inspected that the data processor employs Permido as secure e-mail service.</p> <p>We have inspected that no external services have access to the data processor's network.</p>	No exceptions noted.
Encryption of personal data <ul style="list-style-type: none"> ► The Data Processor 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. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected the data processor's encryption policy for encryption of personal data.</p> <p>We have by samples inspected that encrypted hard drives is established on all computers.</p>	No exceptions noted.

Control area B		
Control Objective ► Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.		
Control activities	Test performed by BDO	Result of test
	We have inspected that the data processor employs Permido as secure e-mail service.	
Firewall <ul style="list-style-type: none"> ► The Data Processor has configured firewall according to best practise. ► The Data Processor only use services/ports which are needed. ► Firewalls are configured and validated periodically when needed, thus, service/ports only are open when needed. 	We have interviewed relevant personnel with the data processor. We have inspected that firewall is configured according to best practice. We have by request been informed that the firewall service on the servers is updated.	No exceptions noted.
Network security <ul style="list-style-type: none"> ► 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 Data Processor's network is segmented so that internal services/servers cannot communicate directly with the internet. ► The Data Processor uses known network technologies and mechanisms (Firewall/Intrusion Detection System/Intrusion Prevention System) to protect internal network. 	We have made inquiries to relevant staff at the data processor. We have inspected the data processor's network topology and observed servers that run applications cannot be accessed directly from the Internet. We have observed that the network is structured according to best practice and that the network is segmented from the guest network. We have on request been informed that all access to the data controller's data is through VPN.	No exceptions noted.
Anti-virus program <ul style="list-style-type: none"> ► Anti-virus software is installed on all servers and workstations. ► Anti-virus software is updated on an ongoing basis and updated with the latest version. 	We have made inquiries to relevant staff at the data processor. We have inspected the data processor's IT security policy and observed that antivirus must be installed on all computers and serves.	No exceptions noted.

Control area B		
Control Objective ► Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.		
Control activities	Test performed by BDO	Result of test
	We have through samples observed that computers and servers have updated antivirus installed.	
Vulnerability scanning and penetration testing <ul style="list-style-type: none"> ► At least once a year, vulnerability scanning/port scanning of the Data Processor's network is performed. The result is documented in a report. ► The Data Processor reviews the report and follows up on ascertained weaknesses. ► The Data Processor processes/handles/mitigates any vulnerabilities based on a risk assessment. ► The Data Processor has documented their handling/mitigation of weaknesses found. 	We have made inquiries to relevant staff at the data processor. We have inspected that the data processor has performed monthly vulnerability scans. We observed a few vulnerabilities has been identified. We have inspected that the data processor's TRUST management has reviewed and accepted the vulnerabilities.	No exceptions noted.
Back-up and re-establishment of data <ul style="list-style-type: none"> ► Back-up of systems and data is performed daily. ► Operation and storage of back-ups are outsourced to sub data processor. ► Restore test is performed once a year. 	We have made inquiries to relevant staff at the data processor. We have inspected the data processor's security policy. We have inspected that back-up of systems are performed daily, weekly, and monthly. We have observed that monthly backup is stored for three months. We have observed that back up restore tests are performed regularly. We have inspected that restore test was performed during the period.	No exceptions noted.
Maintenance of system software	We have made inquiries to relevant staff at the data processor.	No exceptions noted.

Control area B		
Control Objective ► Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.		
Control activities	Test performed by BDO	Result of test
<ul style="list-style-type: none"> ► The Data Processor keeps an overview of operating system software/third party programmes on workstations and servers which is updated continuously. ► Operating system software on servers and workstations is constantly updated. ► The data processor has implemented a system software update process to ensure system availability and security. 	<p>We have inspected that security software is automatically updated through Jamf.</p> <p>We have by samples inspected that system software is updated on all computers and servers.</p>	
Logging in systems, databases, and network, including logging of application of personal data <ul style="list-style-type: none"> ► All successful and failed attempts to access the Data Processor's systems and data are logged. ► All user changes in systems and databases are logged. ► The log is deleted after the determined retention period. ► The Data Processor monitors and logs network traffic. ► Logs are kept for 6 months. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected the data processor's procedure for logging.</p> <p>We have observed that logging is implemented and that all successful and unsuccessful login attempts along with changes and access to personal data are logged.</p> <p>We have observed the data processor monitors and logs network traffic.</p> <p>We have observed that logging is stored for 6 months.</p>	No exceptions noted.
Monitoring <ul style="list-style-type: none"> ► The Data Processor has established a monitor system for monitoring of production environments, including uptime, performance, and capacity. ► The Data Processor is notified of identified alerts and follows up on these. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected the data processor's monitor system.</p> <p>We have observed that the system is monitoring capacity, uptime, and performance.</p> <p>We have inspected that the system notifies alarms, and that the data processor follows up on incidents.</p>	No exceptions noted.

Control area B		
Control Objective		
<p>► Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.</p>		
Control activities	Test performed by BDO	Result of test
<p>Repair and service as well as disposal of IT equipment</p> <ul style="list-style-type: none"> ► The data processor gets IT equipment repaired on-premises and monitors the repair. ► The data processor disposes of IT equipment by physical destruction of data-bearing media. ► The data processor securely deletes data on data-bearing media (overwriting/distortion, encryption) ► The data processor maintains a list of destroyed IT equipment. ► Data processor follows ISO 27001 or NIST 800-88 instructions regarding media disposal. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected disposal, destruction, and reuse policy and observed that media should be destroyed according to best practice.</p> <p>We have by request been informed that no it-equipment has been destroyed or repaired during the period.</p>	<p>We have identified that there has been no disposal of media during the period. Therefore, we cannot test the control for implementation and efficiency.</p> <p>No exceptions noted.</p>
<p>Testing, assessment and evaluation of the efficiency of the technical and organisational security measures</p> <ul style="list-style-type: none"> ► The Data Processor tests, assesses and evaluates the efficiency of whether the technical and organisational security measures are appropriate in relation to the data processed on behalf of the Controller. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected that tests and evaluation of implemented technical and organisational security measures are conducted during the monthly TRUST meetings.</p>	<p>No exceptions noted.</p>
<p>Development and sustainability of systems</p> <ul style="list-style-type: none"> ► The Data Processor works on the basis of privacy-by-design principles in development and maintenance tasks. ► Risk assessment of system changes has been performed to ensure data protection through design and default settings. 	<p>We have made inquiries of relevant personnel at the Data Processor.</p> <p>We have inspected that the data processor works based on privacy-by-design principles observed that the data processor performs risk assessment in situations with development changes.</p> <p>Through random samples we have inspected that all relevant development tasks are risk assessed.</p>	<p>No exceptions noted.</p>

Control area B		
Control Objective		
<p>▶ Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.</p>		
Control activities	Test performed by BDO	Result of test
<p>Information security in development and changes</p> <ul style="list-style-type: none"> ▶ The Data Processor works on security-by-design principles in development and change tasks. ▶ A rollback plan is implemented in case of errors in the production environment. ▶ The Data Processor minimises attack surfaces by relating to functionalities and open service usability in development and modification tasks. ▶ User creation takes place as a starting point with the lowest user rights level. ▶ Only the Data Processor's developers have access to source code. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected that the data processor works based on privacy-by-design principles.</p> <p>We have inspected that the data processor has a plan for rollback of changes.</p> <p>We have observed that user creation is based on lowest user rights level as a starting point.</p> <p>We have observed that only employees with work related needs have access to the source code.</p> <p>We have by samples inspected that the change management procedure is complied with during the period.</p>	<p>No exceptions noted.</p>
<p>Segregation of development, test and production environments</p> <ul style="list-style-type: none"> ▶ Segregation of duties between development and operation has been introduced. ▶ Changes to functionality are tested before being put in operation. ▶ Development and test are performed in development environments, which are segregated from production systems. ▶ A version management system is used to register all changes in source code 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have observed that the data processor has established segregation of duties between development and operation.</p> <p>We have observed that all changes to the platform are registered.</p> <p>We have by samples inspected that the change management procedure is compiled during the period.</p>	<p>No exceptions noted.</p>
<p>Personal data in development and test environments</p> <ul style="list-style-type: none"> ▶ Fictional test data or anonymised data are used in development and test environments. 	<p>We have made inquiries to relevant staff at the data processor.</p>	<p>No exceptions noted.</p>

Control area B		
Control Objective ► Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.		
Control activities	Test performed by BDO	Result of test
	We have inspected that all data is fictional in the test and development environment and is generated by a script.	
Support assignments ► Supporters access and handling of personal data is given based on support tickets and the supports work related need.	We have made inquiries to relevant staff at the data processor. Based on random samples of data processing agreements, we have inspected that there is instruction to support with the data controllers. We have inspected that only employees with a work-related need have access to the data controller's personal data.	No exceptions noted.

Control area C		
Control Objective ► Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.		
Control activities	Test performed by BDO	Result of test
Information Security Policy <ul style="list-style-type: none"> ► The Data Processor has prepared and implemented an information security policy. ► The Data Processor has prepared and implemented a data protection policy. 	We have made inquiries to relevant staff at the data processor. We have inspected the data processor's information security policy. We have inspected the data processor's data protection policy.	No exceptions noted.
Information security policies in compliance with data processing agreements <ul style="list-style-type: none"> ► The management of the data processor makes sure that the information security policy is not in conflict with data processing agreements. 	We have made inquiries to relevant staff at the data processor. We have inspected the information security policy and data processing agreements. We have observed that the information security policy is not in conflict with entered agreements.	No exceptions noted.
Review of the information security policy <ul style="list-style-type: none"> ► The Data Processor's information security policy is reviewed and updated at least once annually. ► The Data Processor's data protection policy is reviewed and updated at least once annually. 	We have made inquiries to relevant staff at the data processor. We have observed that the information security policy is reviewed in 22. August 2024. We have observed that the data protection policy is reviewed in 10. September 2024.	No exceptions noted.
Organisation of information security policy <ul style="list-style-type: none"> ► The Data Processor has documented and established management control of information security. ► The Data Processor has documented and established management control of the data protection policy. 	We have made inquiries to relevant staff at the data processor. We have inspected that management of information security and data protection is described.	No exceptions noted.

Control area C		
Control Objective ► Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.		
Control activities	Test performed by BDO	Result of test
	<p>We have observed that the TRUST group, in which the top management sits, is responsible for information security and data protection.</p> <p>We have observed that all controls in relation to complying with information security policy and data protection policy is managed through an ISMS system.</p>	
Recruitment of employees <ul style="list-style-type: none"> ► The Data Processor performs screening of potential employees before employment. ► The Data Processor performs background check in accordance with the Data Processors procedure and the position, which the candidate is to fill. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected the data processor's procedure for employment and observed that the data processor performs screening of potential employees before employment.</p> <p>We have by inquiry been informed that no new employees have access to personal data. Consequently, we have not been able to test for implementation.</p>	<p>We have identified that there have been no cases of employment with access to personal data during the period. Therefore, we cannot test the control for implementation and efficiency.</p> <p>No exceptions noted.</p>
Resignation of employees <ul style="list-style-type: none"> ► The Data Processor has prepared and implemented a procedure for resignation of employees at the end of the employment. ► At resignation, the employee is informed that the signed confidentiality agreement is still applicable. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected the data processor's terms of employment.</p> <p>Using random samples, we have inspected that the employee's confidentiality agreement is still applicable after resignation.</p>	<p>No exceptions noted.</p>
Training and instruction of employees processing personal data <ul style="list-style-type: none"> ► The Data Processor conducts awareness training of new employees in accordance with data protection and information security, in continuation of the employment. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected that new employees are trained in data protection and GDPR.</p>	<p>We have identified that there have been no cases of employment with access to personal data during the period. Therefore, we cannot test the control for implementation and efficiency.</p> <p>No exceptions noted.</p>

Control area C		
Control Objective ► Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.		
Control activities	Test performed by BDO	Result of test
<ul style="list-style-type: none"> ► The Data Processor conducts introduction courses for new employees regarding how data controllers are to process data. ► The Data Processor conducts training of employees on an ongoing basis in accordance with data protection and information security and handling hereof. 	<p>We have by inquiry been informed that no new employees have access to personal data. Consequently, we have not been able to test for implementation.</p> <p>We have observed that all employees are trained in data protection and information security on an ongoing basis.</p>	
Awareness and information campaigns for employees <ul style="list-style-type: none"> ► The Data Processor conducts awareness training in the form of morning meetings, notices, etc. ► The Data Processor performs information campaigns for employees on data protection and information security. ► The Data Processor performs monthly meetings on processing and protection of personal data protection. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have observed that all employees are trained in data protection and information security on an ongoing basis.</p> <p>We have inspected that the data processor shares information about GDPR and information security regularly.</p> <p>We have inspected that there are monthly meetings in the TRUST management, where initiatives and focus areas are discussed.</p>	No exceptions noted.
Confidentiality and secrecy agreement with employees <ul style="list-style-type: none"> ► All employees are subjected to statutory duty of confidentiality under the provisions of the Danish Criminal Code. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected that the standard employment contract contains a duty of confidentiality.</p> <p>Through random samples we have inspected that employees have signed a confidentiality agreement.</p>	No exceptions noted.
Confidentiality and secrecy agreement with employees <ul style="list-style-type: none"> ► All employees have signed an employment contract, which contains a section regarding confidentiality. ► All employees have signed a confidentiality and secrecy agreement. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected that the standard employment contract contains a duty of confidentiality.</p>	We have identified that processor does not give contractors access to personal data. Therefore, we cannot test the control for implementation and efficiency.

Control area C		
Control Objective ► Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.		
Control activities	Test performed by BDO	Result of test
► External suppliers/consultants are subject to professional secrecy when entering cooperation.	Through random samples we have inspected that employees have signed a confidentiality agreement. We have on request been informed that there have been no external consultants with access to personal data during the period.	No exceptions noted.
Obligations of security of processing and impact assessments. ► Procedures for assistance to the Controller when assisting in relation to articles 32 and 35 have been prepared (article 32 is covered by the risk assessment, and therefore, we focus on procedures for making a DPIA, remember that these should only be made if processing of personal data results in a high risk for the data subjects and their freedom rights. Article 35 (3) states three examples where a DPIA must be made)).	We have made inquiries to relevant staff at the data processor. We have inspected the data processor's procedure for cooperation with the customer's data controller. We have observed that the data processor provides assistance to data controllers in relation to articles 32, 35, and 36. We have by inquiry been informed that the data processor has not provided assistance during the period.	We have identified that the processor has not been asked to assist with obligations pursuant to Article 32-36. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.
Audit and inspection ► The Data Processor is obligated to prepare an ISAE 3000 assurance report on the technical and organisational security measures aimed at processing and protection of personal data. ► The Data Processor assists the Controller at physical supervision by making available resources. ► The Data Processor makes available the information necessary to the Controller and the supervisory authorities upon request, in connection with audit and inspection of the Data Processor.	We have made inquiries to relevant staff at the data processor. We have inspected that the data processor is preparing an ISAE 3000 assurance report. We have been informed that there have been no inquiries regarding further supervision by the data controllers.	We have identified that there have not been any incidents regarding audit or inspection from the data controller. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.
Records of processing activities	We have made inquiries to relevant staff at the data processor.	No exceptions noted.

Control area C		
Control Objective ► Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.		
Control activities	Test performed by BDO	Result of test
<ul style="list-style-type: none"> ► The Data Processor has established a record of processing activities as Data Processor. ► The record is updated with significant changes continuously. ► The record is updated at least once a year during the annual review. 	<p>We have inspected that the data processor has a record of processing activities.</p> <p>We have observed that the record is reviewed in December 2023.</p>	
Storage of the record <ul style="list-style-type: none"> ► The record is stored electronically on the Data Processor's system/file drive. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have observed that the record is stored electronically in the ISMS system.</p>	No exceptions noted.
The Danish Data Protection Agency's access to the record <ul style="list-style-type: none"> ► The Data Processor hands over the record at the request of the Danish Data Protection Agency. 	<p>We have interviewed relevant personnel with the Data Processor.</p> <p>We have been informed that there have been no requests for the record by the Danish Data Protection Agency during the period.</p>	<p>We have identified that the record of processing activities has not been requested during the audit period. Therefore, we cannot test the control for implementation and efficiency.</p> <p>No exceptions noted.</p>
Selection of Data Protection Officer <ul style="list-style-type: none"> ► The Data Processor has developed and implemented a procedure for appointing a Data Protection Officer. ► The Data Processor has appointed a Data Protection Officer. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected that the data processor has entered an agreement with DPO Danmark who will be functioning as DPO.</p> <p>We have inspected that the data processor has appointed a Data Protection Officer in Germany.</p>	No exceptions noted.
The position of the Data protection officer.	<p>We have made inquiries to relevant staff at the data processor.</p>	No exceptions noted.

Control area C		
Control Objective ► Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.		
Control activities	Test performed by BDO	Result of test
<ul style="list-style-type: none"> ► The Data Processor has prepared and implemented a description of the position of the Data Protection Officer. ► The Data Processor engages the Data Protection Officer regarding the protection of personal data. ► The Data Protection Officer reports directly to the Data Processor's management. ► The Data Protection Officer is subject to a duty of confidentiality/confidentiality. 	<p>We have inspected the cooperation agreement with DPO Denmark.</p> <p>We have observed that the agreement contains requirements regarding duty of confidentiality and reporting.</p> <p>We have observed that the German agreement contains requirements regarding duty of confidentiality and reporting.</p>	
Tasks of the Data Protection Officer <ul style="list-style-type: none"> ► The data processor has prepared and implemented a task description of the Data Protection Officer's tasks. ► The Data Protection Officer does not perform other tasks which conflict with the tasks of the Data Protection Officer at the Data Processor. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected the cooperation agreement with DPO Denmark.</p> <p>We have observed that the Data Protection Officer does not perform tasks that conflict with other tasks.</p> <p>We have observed that the German Data Protection Officer does not perform tasks that conflict with other tasks.</p>	No exceptions noted.

Control area D		
Control Objective ► To ensure that the Data Processor can delete and return personal data when the service regarding the processing has terminated, in accordance with instruction from the Controller.		
Control activities	Test performed by BDO	Result of test
Deletion of personal data ► The Data Processor deletes the Controller's personal data per instruction, at termination of the main agreement.	We have made inquiries to relevant staff at the data processor. We have inspected the data processors procedure for termination of the main agreement. We have on request been informed that there has been no termination of contracts with the data controller.	We have identified that there has been no termination of contracts with the data controller. Therefore, we cannot test the control for implementation or efficiency. No exceptions noted.
Return of personal data ► The Data Processor returns the Controller's personal data as per instruction, at termination of the main agreement. ► The data controller and data processor have agreed in which format, transfer and media data is to be returned when requested by the data controller.	We have made inquiries to relevant staff at the data processor. We have inspected the data processors procedure for termination of the main agreement. We have on request been informed that the data processor has not received a request for returning data during the period.	We have identified that there has been no termination of contracts with the data controller. Therefore, we cannot test the control for implementation or efficiency. No exceptions noted.

Control area E		
Control Objective ► Procedures and controls are followed, which ensure that the data processor only stores personal data in accordance with the agreement with the data controller.		
Control activities	Test performed by BDO	Result of test
Storage of personal data <ul style="list-style-type: none"> ► Personal data is retained so it is unavailable for unauthorised personnel. ► The Data Processor's personal data can only be accessed based on one's work-related need. ► Confidential digital personal data is kept in encrypted format. ► Physical material containing personal data is kept sealed. ► Personal data is kept only as long as there is a legitimate reason for the use/storage. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected that personal data is contained so it is only available to employees with work related needs.</p> <p>We have inspected that firewall is set up so that access is through encrypted SSH jump host.</p> <p>We have inspected that no physical material contains personal data.</p> <p>We have inspected that personal data is only stored in accordance with the concluded data processing agreements, which are 12 months after the completion of the process.</p>	<p>No exceptions noted.</p>

Control area F		
Control Objective ► Procedures and controls are followed to ensure that only approved subprocessors are used, and that the data processor, by following up on their technical and organisational measures to protect the data subjects' rights and the processing of personal data, ensures satisfactory processing security.		
Control activities	Test performed by BDO	Result of test
Subprocessor agreement and instruction <ul style="list-style-type: none"> ► When using subprocessors the Data Processor enters into a sub data processing agreement, which assigns the same data protection obligations to the sub processor as the Processor is assigned. ► Instructions from the Controller is disclosed to the sub-processor. ► The data processing agreement with the subprocessor is signed and stored electronically. ► The data processing agreement with the subprocessor contains information about the use of subprocessors. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected that the data processor has entered sub data processing agreements which assigns the same data protection obligations to the subprocessor as the data processor.</p> <p>We have inspected that sub data processing agreements are signed, stored electronically and include contains information about the use of subprocessors.</p>	<p>No exceptions noted.</p>
Approval of sub data processors <ul style="list-style-type: none"> ► The Data Processor only use approved sub processors. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>We have inspected subprocessors in the data processing agreements with the data controllers. We have observed that a subprocessor for backup (Digital Ocean) does not appear in the samples for data processing agreement with the data controllers.</p>	<p>We have identified that the subprocessor for backup (Digital Ocean) does not appear in the samples for data processing agreement with the data controllers.</p> <p>No further exceptions noted.</p>
Changes to approved subprocessors <ul style="list-style-type: none"> ► The Data Processor has prepared an appropriate process with the Controller for change of approved subprocessors. ► The Data Processor communicates to the Controller when changing subprocessors in connection with general approval of subprocessors. ► The Controller may object to changing subprocessor. 	<p>We have made inquiries to relevant staff at the data processor.</p> <p>Upon request, we have been informed that there have been no changes to subprocessors for the existing services during the declaration period.</p>	<p>We have identified that no new sub processors have been taken into use during the period. Therefore, we cannot test the control for implementation and efficiency.</p> <p>No exceptions noted.</p>

Control area F		
Control Objective ► Procedures and controls are followed to ensure that only approved subprocessors are used, and that the data processor, by following up on their technical and organisational measures to protect the data subjects' rights and the processing of personal data, ensures satisfactory processing security.		
Control activities	Test performed by BDO	Result of test
► When changing subprocessor, the Data Processor must have a new preceding specific written approval from the Controller.		
Overview of approved subprocessors ► The Data Processor has an overview of approved subprocessors. Among other things, the overview of approved subprocessors contains information about contact person, location for processing and type of processing and category of personal data, which the subprocessor undertakes.	We have made inquiries to relevant staff at the data processor. We have inspected an overview of the data processor's subprocessors. We have observed that the overview contains name, location, and with what the subprocessor assists the processor.	No exceptions noted.
Supervision of sub processors ► The Data Processor performs supervision, including obtains and reviews the subprocessor's audit opinions, certifications, etc. ► The Data Processor performs supervision of the subprocessor, based on a risk assessment. ► The Data Processor performs supervision of the subprocessor, at least once a year.	We have made inquiries to relevant staff at the data processor. We have inspected an overview of the data processor's subprocessors. We have inspected that the data processor has performed supervision with all subprocessors.	No exceptions noted.

Control area H		
Control Objective ► Procedures and controls are followed, which ensure that the data processor can assist the data controller with the provision, correction, deletion, or restrictions of information on the processing of personal data to the data subject.		
Control activities	Test performed by BDO	Result of test
The data subjects' rights ► The Data Processor has prepared a procedure for assistance to the Controller at fulfilling the data subjects' rights. ► It is possible to provide insight into all information registered in the systems.	We have made inquiries to relevant staff at the data processor. We have inspected procedures for assistance to the controller at fulfilling the data subject's rights. We have observed that the subjects have the right to see the processed data regarding the subjects. We have inspected that request of data deletion is deleted automatically.	No exceptions noted.

Control area I		
Control Objective ► Procedures and controls are followed to ensure that any security breaches can be handled in accordance with the relevant data processing agreement.		
Control activities	Test performed by BDO	Result of test
Communication of personal data breach <ul style="list-style-type: none"> ► The Data Processor communicates to the Controller the personal data breach without undue delay. ► The Data Processor updates the Controller on all information relevant and necessary when the information is available to the Data Processor. ► Communication between Data Processor and Controller is documented and stored. 	We have made inquiries to relevant staff at the data processor. We have inspected procedures for information security breach. We have observed that the data processor has a plan for personal data breach in which the employees' whom to contact appears. We have observed that communication between the data processor and controller is documented, stored, and evaluated. We have observed that there have been no breaches with the data controller's data during the period.	We have identified that the processor has not had any personal data breaches. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.
Identification of personal data breaches <ul style="list-style-type: none"> ► The Data Processor performs surveillance for detecting breaches of the personal data security. ► The Data Processor has prepared a procedure for assessing and identifying personal data breaches. 	We have made inquiries to relevant staff at the data processor. We have inspected procedures for incident management. We have observed that the data processor has instructed the employees in identification of personal data breaches.	We have identified that the processor has not had any personal data breaches. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.
Registration of personal data breaches <ul style="list-style-type: none"> ► The Data Processor registers personal data breaches in the data breach log. ► The Data Processor has prepared and implemented a procedure for experience gathering when personal data is breached. 	We have made inquiries to relevant staff at the data processor. We have inspected that all data breaches are logged. We have inspected that the data processor has prepared and implemented a procedure for personal data breaches.	We have identified that the processor has not had any personal data breaches. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.

Control area I		
Control Objective ► Procedures and controls are followed to ensure that any security breaches can be handled in accordance with the relevant data processing agreement.		
Control activities	Test performed by BDO	Result of test
Assisting the data controller with handling personal data breaches ► Procedures for assistance to the Controller when assisting in relation to articles 33-34 and 36 have been prepared.	We have made inquiries to relevant staff at the data processor. We have inspected procedures for assistance to the Controller in relation to articles 33, 34 and 36. We have been informed that no incidents regarding assistance to the Controller in case of personal data breach has occurred during the period.	We have identified that the processor has not had any personal data breaches. Therefore, we cannot test the control for implementation and efficiency. No exceptions noted.

**BDO STATSATORISERET
REVISIONSAKTIESELSKAB**

**HAVNEHOLMEN 29
1561 KØBENHAVN V**

CVR NO. 20 22 26 70

BDO Statsautoriseret revisionsaktieselskab, a Danish limited liability company, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO in Denmark employs more than 1,800 people and the worldwide BDO network has more than 120,000 partners and staff in 166 countries.

Copyright - BDO Statsautoriseret revisionsaktieselskab, CVR No. 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 STATS-AUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670

Partner

Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff

IP: 77.243.xxx.xxx

2025-05-01 11:54:05 UTC



Dette dokument er underskrevet digitalt via [Penneo.com](https://penneo.com). De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptografiske beviser er indlejret i denne PDF for validering i fremtiden.

Dette dokument er forseglet med et kvalificeret elektronisk segl med brug af certifikat og tidsstempel fra en kvalificeret tillidstjenesteudbyder.

Sådan kan du verificere, at dokumentet er originalt

Når du åbner dokumentet i Adobe Reader, kan du se, at det er certificeret af **Penneo A/S**. Dette beviser, at indholdet af dokumentet er uændret siden underskriftstidspunktet. Bevis for de individuelle underskrivers digitale underskrifter er vedhæftet dokumentet.

Du kan verificere de kryptografiske beviser vha. Penneos validator, <https://penneo.com/validator>, eller andre valideringstjenester for digitale underskrifter.