Dansk Revision Århus
godkendt revisionsaktieselskab
Tomsagervej 2
DK-8230 Åbyhøj
aarhus@danskrevision.dk
www.danskrevision.dk
Telefon: +45 89 36 12 12
Telefax: +45 89 36 12 00
CVR: DK 26 71 76 71
Bank: 6181 0007769555

DIGIREHAB A/S

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with DigiRehab A/S' clients.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

GGi INDEPENDENT MEMBER

Table of Contents

1. Management's statement 3
2. Independent auditor's report 5
3. Description of processing 7
4. Control objectives, control activity, tests and test results 13

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

1. Management's statement

DigiRehab A/S processes personal data for its clients (data controller), in accordance with data processing agreements.

The accompanying description has been prepared for the data controller, who has used DigiRehab's services, and who has a sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the EU Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "the Regulation") have been complied with. DigiRehab A/S confirms that:

a) The accompanying description, fairly presents DigiRehab's services and systems, which has processed personal data for the data controllers subject to the Regulation throughout the period from 1st of September 2024 to 31st of August 2025. The criteria used in making this statement were that the accompanying description:

   (i) Presents how DigiRehab's services and systems was designed and implemented, including:

   - The types of services provided, including the type of personal data processed
   - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete and restrict 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
   - Controls that we, in reference to the scope of DigiRehab's services, have assumed would be implemented by the data controllers and which, if necessary in order to achieve the control objectives stated in the description, are identified in the description

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

- Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data

(ii) Includes relevant information about changes in the Data Processor's services, in the processing of personal data in the period from 1st of September 2024 to 31st of August 2025.

(iii) Does not omit or distort information relevant to the scope of DigiRehab's services being described for the processing of personal data while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of DigiRehab's services that the individual data controllers might consider important in their particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were, in our view, suitably designed and operated effectively throughout the period from 1st of September 2024 to 31st of August 2025. The criteria used in making this statement were that:

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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1st of September 2024 to 31st of August 2025.

c) Appropriate technical and organisational safeguards were established and maintained to comply with the agreements with the data controllers, sound data processing practices and relevant requirements for data processors in accordance with the Regulation.

Viborg, 7. november 2025

Niels Heuer, CEO

DigiRehab A/S
Brovej 20 A, st.
8800 Viborg

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

2. Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with DigiRehab's clients using the related services.

To: DigiRehab A/S and DigiRehab A/S´ clients using the related services.

Scope

We were engaged to provide assurance about DigiRehab's description of services in relation to the processing of personal data, in accordance with the data processing agreement with DigiRehab's clients as the data controller, throughout the period from 1st of September 2024 to 31st of August 2025. As well as provide assurance as to the design and effectiveness of controls related to the control objectives stated in the description.

We express reasonable assurance in our conclusion.

DigiRehab A/S' responsibilities

DigiRehab A/S is responsible for preparing the description and the accompanying statement on page 3-4, including the completeness, accuracy, and the method of presentation of the description and statement, 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 independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by FSR - Danish Auditors (Code of Ethics for Professional Accountants), which are based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional conduct.

Dansk Revision Aarhus is subject to the International Standard on Quality Control (ISQC 1) and accordingly uses and maintains a comprehensive system of quality control, including documented policies and 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 DigiRehab's description and on the design and effectiveness of controls related to the control objectives stated in that description, based on our procedures.

We conducted our engagement in accordance with International Standard on Assurance Engagements 3000, "Assurance Engagements Other than Audits or Reviews of Historical Financial Information", and additional requirements under Danish audit regulation, to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls are appropriately designed and operating effectively.

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 of its services and about the design and operating effectiveness of 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 appropriateness of the criteria specified by the data processor.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

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

DigiRehab A/S' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of DigiRehab's services that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect personal data breaches. Furthermore, the projection of any evaluation of the operating effectiveness 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 management's statement section. In our opinion, in all material respects:

(a) The description fairly presents DigiRehab's processing of personal data, as this was designed and implemented, as of the 1st of September 2024 to 31st of August 2025, and

(b) The controls related to the control objectives stated in the description were appropriately designed as of the 1st of September 2024 to 31st of August 2025; and

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period from 1st of September 2024 to 31st of August 2025.

Description of tests of controls

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

Intended users and purpose

This report and the description of tests of controls, as outlined in section 4, are intended only for data controllers who have used DigiRehab's services, who have a sufficient understanding to consider it along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the Regulation have been complied with.

Åbyhøj, 7. november 2025

Dansk Revision Aarhus
godkendt revisionspartnerselskab, CVR-nr. 26717671

Claus Guldborg Nyvold
Registered Accountant

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

3. Description of processing

DigiRehab A/S provides SaaS solutions for municipalities and private-sector suppliers, that allow them to physically train citizens. Is responsible for procedures and controls that ensure compliance with the processing agreements with their clients. This also covers securing the client's data, operational considerations and maintenance, and finally the further development of the provided solution.

DigiRehab A/S is responsible for implementing, supporting and operating DigiRehab's SaaS solutions www.digirehab.xx and Digidetect, while hosting and backup is handled by a subcontractor.

DigiRehab was established in 2014 and specializes in physical rehabilitation of senior citizens, and with the development of their web-based solution they make these competencies available for Danish municipalities and private actors, that also work in the same industry. DigiRehab's solution is accessible with the client's own IT equipment (primarily tablets). This allows the client to provide tailored in-home assistance.

DigiRehab A/S places great focus on further development of the solution, according to the needs of the client, the end user and society, and therefore has the following vision and mission:

Our vision is to ensure quality of life and independence for as many elderly as possible, despite possible reduced functional capacity. We ensure this by offering a high-quality training tool, which we disseminate with deep insight and evidence of the results.

Our mission is to create welfare technology products that optimize the use of resources in municipal rehabilitation and at the same time increase the quality of life and self-reliance of the elderly.

Nature of processing

The data processor provides, supports and implements the online solution. Data put into the solution by the data controller is hosted by the data processor's use of sub-data processors.

The typical process is thus:

The citizen is selected on the basis of a professional assessment of the rehabilitation potential. The citizen is then created in DigiRehab with master data containing name and CPR / identification number.

The citizen is screened for physical ability and need for help using a professional assessment and physical tests. This information is stored at www.digirehab.dk.

The system creates a training program based on the above information. After this, approx. two training sessions are scheduled per week. After each workout, information is logged about the time of the workout, the citizen's experience (e.g. in case of pain) and the employee assesses the workout on a scale.

The system notifies relevant personnel (e.g. the visitation/medical assessor) about the development of the training efforts and this information is used to assess the further progress.

Intensive training typically ends after 12 weeks, after which maintenance training is started. Data on citizens is stored for up to 5 years or until the end of the main agreement.

The data processor processes this data as well as data about the citizen's assigned services and their development on behalf of the data controller. The latter data comes from the data controller and is used to assess the economic potential of using the system.

The data processor regularly prepares reports about this in anonymized form.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Personal data

General personal data: Name, address, training schedule, screening information regarding the citizen's needs, screening information regarding the citizen's physical capabilities, assessed medical services.

Sensitive personal data: Data regarding health information

Sensitive personal data: CPR number

Categories of data subjects falling within the data processing agreement:

- Citizens receiving services from the health and welfare system, selected based on a professional assessment of rehabilitation potential
- Municipal employees

Practical measures

Appropriate technical and organizational measures have been implemented to secure the processing of personal data. These measures are implemented on the basis of recognized industry standards and guidelines from the data protection regulation and the supervisory authority.

Handling of information security and processing of personal data

Through the central information security policy and internal personal data policy, the management has described Digi-Rehab A/S' structure for information security and processing of personal data. As a minimum, the policies must be revised once a year.

DigiRehab A/S' overall goal is to deliver a stable and secure SaaS solution to clients. To support this, policies and procedures have been introduced to ensure that deliveries are consistent and transparent.

DigiRehab A/S' internal guidelines for information security and processing of personal data apply to all employees and to all deliverables.

All servers and network devices are handled by the hosting provider, which is audited by an external auditor at least once a year.

The internal guidelines are formalized such that DigiRehab A/S has one common set of rules. In this way, a stable operating environment is achieved, a high level of security and requirements in data processing agreements are met.

Employees and training

Management is tasked with ensuring that competences are maintained and that the company's guidelines are complied with. DigiRehab A/S follows normal guidelines for handling personnel. Management requires that all employees and subcontractors maintain information security in accordance with DigiRehab A/S' policies and procedures.

All employees and relevant business partners are regularly informed and made aware of DigiRehab A/S' guidelines for information security and processing of personal data. The guidelines, which also apply after termination or change of employment, are defined and communicated to the employee/supplier and are enforced by the company.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Physical security and environmental protection

DigiRehab's A/S office facilities are secured with an alarm outside the office's opening hours. The alarm is connected to a manned alarm control center with emergency response. Outside office opening hours, only authorized personnel have access to the facilities. In addition, access to confidential material that is stored physically is secured in locked cabinets, and access to this is limited to selected employees.

Network security

The company does not store operational data in the office's facilities, as operational data is stored by the hosting partner. Internet to the office facilities is fiber, and the server is protected with a firewall.

Operating environment

DigiRehab A/S' operating environment is located in the subcontractor's data center, where the latter is responsible for ensuring security in accordance with contractual requirements.

The subcontractor has extensive experience in the construction and operation of data centers, and is responsible for the physical security, fire and water damage detection as well as power and cooling.

User management/Secure access

The management has established guidelines for the administration of access to both the internal operating environment and to the production environment, including the allocation of rights, so that an appropriate separation of duties has been established. Access to the various IT environments takes place by specifying a unique user ID and associated password.

PC

All employees follow password and screen saver procedures.

Clients who use DigiRehab, use a login procedure via their own ADFS, where they themselves manage user access and password requirements. Login attempts are logged. In the event of a failed attempt, the DigiRehab administrator can see the reason for this and notify the clients' technical department, who can associate the user with the correct ADFS groups. The log is automatically deleted after 6 months.

Regarding user creations or password resets (where the client does not use ADFS), users must have a secure, temporary password that must be changed immediately after initial use. The temporary password must be unique and follow best practice.

Antivirus/Malware protection

Management has established guidelines for PC protection against malware and viruses.

Itpilot A/S is responsible for and manages antivirus and malware protection on DigiRehab A/S' servers in accordance with contractual requirements.

Monitoring

Itpilot A/S is responsible for and administrates monitoring of DigiRehab A/S' servers, data storage, network units, etc.

Backup

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Itpilot A/S is responsible for and manages the backup of DigiRehab A/S' operating environment in accordance with contractual requirements.

Patch Management

Itpilot A/S is responsible for and manages patches on DigiRehab A/S' operating environment in accordance with contractual requirements.

Change Management

The purpose of change management is to ensure that changes are tested before changes are push into production.

The procedure for change management starts when a need for a change arises. The change is registered in the DevOps task management system. When a change is to be made, it is passed on as a task to a programmer. The programmer performs the change on a local copy of the server. When the programmer has developed/corrected, the programmer themselves tests their correction. When the programmer is satisfied with the result, the solution is uploaded to the test server, where the functions of the change are reviewed and evaluated.

This continues as an iterative process until the changes meet the desired result, and they are subsequently ready to be uploaded to the production server and made available to DigiRehab A/S' clients. Uploading to the operation server is done periodically and outside working hours.

Managing IT security incidents

All employees of DigiRehab A/S are familiar with procedures and reporting of various types of incidents and weaknesses that may affect the safety of DigiRehab A/S' operations. Security incidents and weaknesses must be reported to the IT administrator as soon as possible. The IT administrator, together with the management, is responsible for defining and coordinating a structured administrative process that ensures an appropriate response to security incidents.

Disaster and business continuity planning

The purpose of disaster and BCP at DigiRehab A/S is to ensure business continuity and to provide clients with a quick re-establishment of services in the event of a system breakdown.

DigiRehab's hosting supplier itpilot ApS is responsible for monitoring and operating the system. Physical and digital attacks on and re-establishment of the system will therefore follow the hosting supplier's contingency plan.

In the event of major breakdowns, clients or the clients' DPO who use the affected services are informed via mailing list. This message contains a preliminary status, error description and, if possible, an estimate for when the error will be corrected. Clients are kept continuously informed through a mailing list until the error is rectified.

Compliance with the role of data processor

DigiRehab A/S enters into data processing agreements with all clients before the client's use of the DigiRehab SaaS solution begins.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

DigiRehab A/S complies with the security requirements set out in Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 (hereinafter the Data Protection Regulation) and the Data Protection Act.

DigiRehab A/S keeps records of the processing of personal data as well as records of all breaches of personal data security.

DigiRehabs A/S' processing of personal data on behalf of the clients takes place exclusively according to documented instructions, unless - otherwise required according to EU law or the national law of the member states to which DigiRehab A/S is subject; in that case, DigiRehab A/S informs the client of this legal requirement before processing, unless the applicable law prohibits such notification for reasons of important societal interests.

DigiRehab A/S and their employees are prohibited from obtaining information of any kind that is not relevant to the performance of their duties.

DigiRehab A/S immediately informs the client of any breach of personal data security.

The client decides whether to delete or return the personal data after the processing of the personal data has completed.

All employees are made aware of the guidelines and are continuously trained accordingly.

Risk assessment

For each processing activity, an assessment has been made of the likelihood of a loss of confidentiality (unauthorized persons gaining access to the information), integrity (the information is incorrect) or availability (information is lost). This assessment is based on threats and the measures implemented to protect the confidentiality, integrity and availability of the information.

Next, the consequences for those registered have been assessed. This assessment is based on what the consequence for the data subject is if there is a loss of confidentiality, integrity or the availability of the information. Assessment is based on whether the information is general, special or sensitive and the possible indirect consequences regarding the type of data set. The greater the probability that the information's loss of confidentiality, integrity or availability may lead to material or immaterial damage to the data subject, the greater the consequence.

We refer to section 4, where the specific control activities are described.

Complementary controls at the data controllers

This general description does not take into account, any specific client agreements.

Most client grant access to DigiRehab by integrating with the client's ADFS solution. This means that the client controls which employees have access to the client's data in the DigiRehab solution. These clients therefore bear full responsibility for handling this access, as it gives access to any confidential information. This means that DigiRehab A/S is not responsible for access rights, including allocation, change and termination, in relation to the individual client's users and their access to DigiRehab. The client is obliged to ensure the necessary controls in connection with this control objective.

The client is therefore responsible for ensuring that their employees have access to the system and that they protect the information that is registered.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

The following is a description of the controls which are expected to be implemented by the data controllers and which are essential to achieve the control objectives listed in section 4.

The data controller has the following obligations:

- to ensure that the personal data is up to date
- to make sure that the instruction is legal in relation to the personal data law regulation applicable at any time
- that the instruction is appropriate in relation to this data processing agreement and the main service.
- to ensure that the data controller's users are up-to-date

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

4. Control objectives, control activity, tests and test results

Control objective A **Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistently with the data processing agreement entered into.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
A.1	Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that there are formalized procedures that ensure that processing of personal information only takes place in accordance with instructions. Inspected that the procedures contain requirements for a minimum annual assessment of the need for updating, including changes in the data controller's instructions or changes in data processing. Inspected that the procedures have been updated.	No exceptions noted.
A.2	The data processor only processes personal data as stated in the instructions from the data controller.	Inspected that processing of personal data only takes place in accordance with instructions.	No exceptions noted.
A.3	The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions.	Inspected that there are formalized procedures that ensure that the processing of personal information does not go against the data protection regulation or other legislation. Inspected that there are procedures for notifying the data controller in cases where the processing	No exceptions noted.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective A **Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistently with the data processing agreement entered into.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
		of personal data is deemed to be in breach of the legislation. Inspected that the data controller is notified in cases where the processing of personal data is assessed to be in breach of the legislation.	

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective B **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing**.			
Nr.	Data processor's control activity	Test performed by auditor	Result of auditor's test
B.1	Written procedures exist which include a requirement that safeguards are established for the processing of personal data in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that there are formalized procedures that ensure that the agreed security measures are established. Inspected that procedures are up to date. Inspected safeguards agreed in data processing agreements have been established.	No exceptions noted.
B.2	The data processor has performed a risk assessment and, based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of safeguards, as required by the data controller.	Inspected that there are formalized procedures that ensure that the data processor carries out a risk assessment to achieve adequate security. Inspected that the risk assessment carried out is up to date and takes into account, the current methods of processing of personal data. Inspected that the data processor has implemented the technical measures that ensure adequate security in accordance with the risk assessment. Inspected that the data processor has implemented the security measures as agreed with the data controllers.	No exceptions noted.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective B **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing**.			
Nr.	Data processor's control activity	Test performed by auditor	Result of auditor's test
B.3	For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.	Inspected that antivirus software has been installed for the systems and databases used to process personal information. Inspected that antivirus software is up to date.	No exceptions noted.
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall and VPN.	Inspected that external access to systems and databases used for processing personal data only takes place through a firewall. Inspected that VPN is necessary when logging onto systems remotely.	No exceptions noted.
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	Inquired whether internal networks are segmented in order to ensure limited access to systems and databases used for processing personal data.	No exceptions noted.
B.6	Access to personal data is restricted to only users with a work-related need for such access. Users are uniq. Users with privileged rights are restricted to only users with work-related need for such access.	Inspected that there are formalized procedures for restricting users' access to personal data. Inspected that there are formalized procedures for follow-up that users' access to personal data is in accordance with their work-related needs.	No exceptions noted.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective B **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.**			
Nr.	Data processor's control activity	Test performed by auditor	Result of auditor's test
		Inspected that the technical measures in the application support the limitation in the users' work-related access to personal data. Inspected by a sample of 5 clients, that user access to data is limited to the employees work-related needs. Inspected that all users are uniq. Inspected that privileged rights are limited to employees with a work-related need.	
B.7	For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.	Inspected that systems and databases used for processing personal data have system monitoring with alarms enabled.	No exceptions noted.
B.8	Effective encryption is applied when transmitting special and sensitive personal data through the internet or by email.	Inspected that there are formalized procedures that ensure that the transmission of sensitive and special information over the Internet is protected by strong encryption based on a recognized algorithm. Inspected that technological solutions for encryption have been available and activated throughout the report period.	No exceptions noted.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective B **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.**			
Nr.	Data processor's control activity	Test performed by auditor	Result of auditor's test
		Inspected that encryption is used for transmissions of sensitive and special personal information via the Internet or by e-mail. Inquired whether there have been unencrypted transmissions of sensitive and special personal information during the report period, as well as whether the data controllers have been duly informed about this.	
B.9	Logging of the following events has been established in systems and databases: • Logins and failed attempts to login • Accessing data related to citizens and training programs. • When an employee or administrator, at the client, gives themselves access to a new area	Inspected that there are formalized procedures for setting up logging of user activities in systems and databases used for processing personal data. Inspected that logging of user activities in systems and databases used for processing and transmission of personal data is configured and activated. Inspected that collected information about user activity is protected against manipulation and deletion.	No exceptions noted.
B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's intended purpose according to agreement, and on the data controller's behalf.	Inspected that there are formalized procedures for the use of personal data for development, testing and the like, which ensure that the use only takes place in pseudonymized or anonymized form.	We found non-anonymized test data in the test database, due to an error in updating the test database. We observed the data processor deleting the non-anonymized test data.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective B **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.**			
Nr.	Data processor's control activity	Test performed by auditor	Result of auditor's test
		Inspected, that there are anonymized data in test databases.	
B.11	The technical measures established are tested on a regular basis with vulnerability scans.	Inspected that there are formalized procedures for ongoing tests of technical measures, including the implementation of vulnerability scans. Inspected, that there are performed vulnerability scans in the audit period.	No exceptions noted.
B.12	Changes to systems or databases are made consistently with procedures that ensure maintenance using relevant updates and patches, including security patches. Changes to systems or databases are approved and tested on test servers before they are deployed in production environment. Development is subject to proper security requirements.	Inspected that there are formalized procedures for handling changes to systems and databases, including handling relevant updates, patches and security patches. Inquired, that supplier has the responsibility for patching servers. Inspected that there are formalized procedures for approving and testing changes to systems and databases Inspected that changes to systems and databases are approved and tested before they are deployed to production.	No exceptions noted.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective B **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.**			
Nr.	Data processor's control activity	Test performed by auditor	Result of auditor's test
		Inspected that there are formalized procedures for secure development.	
B.13	A formalised procedure is in place for granting and removing a user's access to personal data. User access needs are assessed on a regular basis, including the continued justification of rights by a work-related need.	Inspected that there are formalized procedures for granting and terminating users' access to systems and databases used for processing personal data. Inspected by a sample of 5 clients, it is ensured that only employees with work-related needs are granted access to the client. Inspected by a sample of 5 terminated employees, that their access to systems and databases is deactivated or removed in a timely manner. Inspected that there is documentation for regular - at least once a year - assessment and approval of assigned user access.	No exceptions noted.
B.14	Systems and databases processing personal data are only accessed via two-factor authentication. Passwords are hashed.	Inspected that users' access to processing of personal data can only be done by using two-factor authentication. Inspected that passwords are hashed.	No exceptions noted.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective B **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing**.			
Nr.	Data processor's control activity	Test performed by auditor	Result of auditor's test
B.15	Physical access safeguards have been established to ensure that only authorised persons can access data centers or personal data.	Inspected that there are formalized procedures that ensure that only authorized persons can gain physical access to data centers in which personal data is stored and processed. Inspected that office facilities are locked outside of working hours. Inspected that clean desk and screen lock is part of the awareness training.	No exceptions noted.
B.16	The data processor has an operational Business Continuity Plan and incident response plans established. The Business Continuity Plan is tested annually.	Inspected that there are established operational Business Continuity Plan and incident response plans Inspected that the Business Continuity Plan is tested in the audit period.	No exceptions noted.
B.17	Application servers and databases are backed up and restore tested.	Inspected procedures for backup and restore test of application servers and databases. Inspected that application servers and databases are backed up. Inspected that backups are restore tested.	No exceptions noted.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective B **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing**.			
Nr.	Data processor's control activity	Test performed by auditor	Result of auditor's test
B.18	The data processor has secure disposal or re-use of equipment.	Inspected procedures for secure disposal or re-use of equipment. Inquired if secure disposal or re-use of equipment has been practiced.	No exceptions noted.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective C **Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
C.1	Management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The IT security policy is based on the current risk assessment. Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.	Inspected that there is an information security policy that management has reviewed and approved within the past year. Inspected documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No exceptions noted.
C.2	Management of the data processor has ensured that the information security policy does not conflict with data processing agreements entered into previously.	Inspected that the information security policy generally meets the requirements for security measures and processing security in concluded data processing agreements. Inspected that the requirements in the data processing agreement entered into with the clients are covered by the information security policy's requirements for security measures and processing security.	No exceptions noted.
C.3	The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant: • References from former employers • Certificates of criminal record • Diplomas • Name and current address	Inspected that there are formalized procedures that ensure verification of the data processor's employees in connection with employment. Inquired that all new employees in the audit period as been screened according to the procedures.	No exceptions noted.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective C **Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
C.4	Upon employment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data. Employees are made aware that there will be sanctions if they do not comply with intern policies and procedures.	Inspected that all hired employees during the report period have signed a confidentiality agreement. Inspected that at sample of 1 new employee have been introduced to the information security policy and procedures for data processing. Inspected that employees are made aware that there will be sanctions if they do not comply with internal policies and procedures.	No exceptions noted.
C.5	For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned. The data processor has a list of it-assets and their owners as well as a procedure for acceptable use of these assets.	Inspected procedures that ensure that resigned employees' rights are deactivated or removed upon termination, and that assets such as access cards, PCs, mobile phones, etc. are seized Inspected that all resigned employees and third party contractors, during the report period, have had their rights removed or accounts deactivated or terminated, and that assets have been withdrawn. Inspected that there is an updated list of it-assets and their owners. Inspected that there are procedures for acceptable use of it-assets.	No exceptions noted.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective C **Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	Inspected that there are formalized procedures that ensure that terminated employees are made aware of the confidentiality agreement and general confidentiality requirements. Inspected that all resigned or dismissed employees during the assurance period that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality.	No exceptions noted.
C.7	Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data. Reporting of security incidents is part of the awareness training.	Inspected that the data processor offers awareness training to employees covering general IT security and processing security in relation to personal data, as well as reporting of security incidents. Inspected documentation that all employees who have either access to or process personal data have completed the awareness training provided.	No exceptions noted.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective D **Procedures and controls are complied with to ensure that personal data can be deleted or returned if arrangements are made with the data controller to this effect.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
D.1	Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that there are formalized procedures for the storage and deletion of personal information in accordance with the agreement with the data controller. Inspected that the procedures are up to date.	No exceptions noted.
D.2	The following specific requirements have been agreed upon, with respect to the data processor's storage periods and deletion routines: • Upon termination of the service regarding the processing of personal data, the data processor must either delete or return the personal data in accordance with provision 11.1, unless the data controller – after signing these provisions – has changed the data controller's original choice. Such changes must be documented and stored in writing, including electronically, as specified in the Regulations.	Inspected that the existing procedures for storage and deletion contain the specific requirements for the data processor's storage periods and deletion routines. Inspected that there is documentation that personal information is stored in accordance with the agreed storage periods.	No exceptions noted.
D.3	Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been: • Returned to the data controller; and/or • Deleted if this is not in conflict with other legislation.	Inspected that there are formalized procedures for processing the data controller's data when the processing of personal data ceases. Inspected by a sample of 0 ceased data processing agreements during the report period,	No exceptions noted.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective D **Procedures and controls are complied with to ensure that personal data can be deleted or returned if arrangements are made with the data controller to this effect.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
		that there is documentation that the agreed deletion or return of data has been carried out.	

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective E **Procedures and controls are complied with to ensure that the data processor will only store personal data in accordance with the agreement with the data controller.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
E.1	Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that there are formalized procedures for the storage and processing of personal data only in accordance with the data processor agreements. Inspected that the procedures are up to date.	No exceptions noted.
E.2	Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.	Inspected that the data processor has a comprehensive and up-to-date overview of processing activities with an indication of locations, countries or land areas.	No exceptions noted.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective F **Procedures and controls are complied with to ensure that only approved sub-data processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
F.1	Written procedures exist which include requirements for the data processor when using sub-data processors, including requirements for sub-data processing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that there are formalized procedures for the use of sub-data processors, including requirements for sub-data processor agreements and instructions. Inspected that the procedures are up to date.	No exceptions noted.
F.2	The data processor only uses sub-data processors to process personal data that have been specifically or generally approved by the data controller.	Inspected that the data processor has a comprehensive and up-to-date overview of used sub-data processors. Inspected that all sub-processors from the data processor's overview of sub-processors, that there is documentation that the sub-processor's data processing appears in the data processor agreements - or is otherwise approved by the data controller.	No exceptions noted.
F.3	When changing the generally approved sub-data processors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the data processor. When changing the specially approved sub-data processors used, this has been approved by the data controller.	Inspected that there are formalized procedures for notifying the data controller of changes in the use of sub-data processors. Inspected documentation that the data controller is notified of changes in the use of sub-data processors during the report period.	No exceptions noted.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective F **Procedures and controls are complied with to ensure that only approved sub-data processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
F.4	The data processor has subjected the sub-data processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	Inspected that there are signed sub-data processor agreements with used sub-data processors, which appear from the data processor's overview. Inspected that all sub-data processor agreements contain the same requirements and obligations as stated in the data processor agreements between the data controllers and the data processor.	No exceptions noted.
F.5	The data processor has a list of approved sub-data processors containing the following details: • Name • CVR number • Address • Description of data processing	Inspected that the data processor has a comprehensive and up-to-date overview of used and approved sub-data processors. Inspected that the overview contains, at a minimum, the required information about the individual sub-data processors.	No exceptions noted.
F.6	Based on an updated risk assessment of each sub-data processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the sub-data processor.	Inspected that there are formalized procedures for follow-up on processing activities by the sub-data processors and compliance with the sub-data processor agreements. Inspected documentation that a risk assessment has been carried out of the individual sub-data	No exceptions noted.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective F **Procedures and controls are complied with to ensure that only approved sub-data processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
		processor and the current processing activity of this. Inspected documentation that proper follow-up has been carried out on technical and organizational measures, the processing security of the sub-processors used, third country transfer basis and the like.	

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective G **Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
G.1	Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that there are formalized procedures that ensure that personal data is only transferred to third party countries or international organizations in accordance with an agreement with the data controller on the basis of a valid transfer basis. Inspected that the procedures are up to date.	Personal data is not transferred to unsecure third countries.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective H **Procedures and controls are complied with to ensure that the data processor can assist the data controller in handing out, correcting, deleting or restricting information on the processing of personal data to the data subject.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
H.1	Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that there are formalized procedures for the data processor's assistance by the data controller in relation to the rights of the data subjects. Inspected that the procedures are up to date.	No exceptions noted.
H.2	The data processor has established procedures in so far as this was agreed that enable timely assistance to the data controller in handing out, correcting, deleting or restricting or providing information about the processing of personal data to data subjects.	Inspected that the available procedures for assistance to the data controller contain procedures for: • Disclosure of information • Correction of information • Deletion of information • Restriction of processing of personal data • Information on the processing of personal data for the data subject. Inspected documentation that the systems and databases used support the implementation of the mentioned procedures.	No exceptions noted.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective I **Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
I.1	Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that there are formalized procedures that contain requirements for notifying the data controllers in the event of a breach of personal data security. Inspected that the procedure is up to date.	No exceptions noted.
I.2	The data processor has established the following controls to identify any personal data breaches: • Employee awareness • Monitoring of the IT environment • Logging of user activities in the system	Inspected that the data processor offers awareness training to employees in relation to the identification of possible breaches of personal data security. Inspected documentation for monitoring the IT environment. Inspected documentation for logging user activities in the system.	No exceptions noted.
I.3	If any personal data breach occurred, the data processor informed the data controller without undue delay and no later than 48 hours after having become aware of such personal data breach at the data processor or a sub-data processor.	Inspected that the data processor has an overview of security incidents with an indication of whether the individual incident has resulted in a breach of personal data security. Asked the sub-data processors if they have detected any breach of personal data security during the report period Inspected that the data processor has included any breaches of personal data security by sub-	No exceptions noted.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Control objective I **Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
		data processors in the data processor's overview of security incidents.	
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency: • The nature of the breach of personal data security • Probable consequences of the breach of personal data security • Measures taken or proposed to be taken to deal with the breach of personal data security.	Inspected that the existing procedures for notifying the data controllers in the event of a breach of personal data security contain detailed procedures for: • Description of the nature of the breach of personal data security • Description of probable consequences of the breach of personal data security • Description of measures taken or proposed to be taken to deal with the breach of personal data security. Inspected documentation that the existing procedures support that measures are taken to handle the breach of personal data security.	No exceptions noted.

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

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."

Niels Heuer
Direktør
Serienummer: d5bdbff9-834a-4442-9665-1ddb5fac0d04
IP: 188.228.xxx.xxx
2025-11-07 15:18:05 UTC

MitID

Claus Guldborg Nyvold
DANSK REVISION ÅRHUS, GODKENDT REVISIONSPARTNERSELSKAB CVR: 26717671
Registreret revisor
Serienummer: 6ab17a51-67d6-4a70-8939-8d28f439a780
IP: 188.120.xxx.xxx
2025-11-10 06:36:10 UTC

MitID

Penneo dokumentnøgle: SKC6E-ON46L-49FSC-PPP08-OS1P0-7II9Z

Dette dokument er underskrevet digitalt via **Penneo.com**. De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptofrafiske beviser er indlejret i denne PDF for validering i fremtiden.

Dette dokument er forseglet med et kvalificeret elektronisk segl. For mere information om Penneos kvalificerede tillidstjenester, se **https://eutl.penneo.com**.

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 underskriveres digitale underskrifter er vedhæftet dokumentet.

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