

Fortes Nordic A/S

Vindegade 34, 1.
5000 Odense C
CVR.NR. 26 82 97 98

ISAE 3000, type 1

Independent auditor's ISAE 3000 assurance report on the description
of controls aimed at information security and processing of personal
data as per May 4th 2026



Contents

1. Management's statement	2
2. Description of Processing	4
3. Independent auditor's ISAE 3000 assurance report on the description of controls aimed at information security and processing of personal data	7
4. Control objectives, control activity, test and test results.....	9

S.nr. 302482

AOG/JR

1. Management's statement

Fortes Nordic A/S processes personal data on behalf of our costumers, who act as data controllers with reference to the data processing agreements.

The accompanying description has been prepared for the data controllers, who uses Fortes Nordic A/S' Project and Portfolio Management, 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.

Fortes Nordic A/S uses Microsoft as a sub-processor for the hosting, web and services applied. The report uses the carve-out method and does not include control objectives and related controls performed by Microsoft.

Fortes Nordic A/S confirms, that:

- a) The accompanying description, in section 2, provides an accurate description of Fortes Nordic A/S Project and Portfolio Management, that processes personal data for data controllers covered by the Regulation as per May 4th 2026. The criteria used in making this statement were that the accompanying description:
 - (i) Presents how Fortes Nordic A/S systems were 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 controllers;
 - The procedures ensuring that the persons authorized 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, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;
 - Controls that we 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;
 - 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) Does not omit or distort information relevant to the scope of the service 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 the service 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 suitably designed and implemented as per May 4th 2026. The criteria used in making this statement were that:
 - (i) The risks that threatened the 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
- c) Appropriate technical and organizational 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.

Odense, May 4th 2026
Fortes Nordic A/S

Karsten Ley Poulsen
Managing Director

2. Description of Processing

2.0 About Fortes Nordic A/S

Fortes Nordic A/S is a Danish software company specializing in project and portfolio management solutions. One of the company's product for Project and Portfolio Management, Fortes Fortes Nordic (hereinafter "Fortes Nordic"), is a cloud-based platform designed to help organizations plan, execute, and monitor projects efficiently.

2.1 Introduction

The purpose of this description is to provide information to customers of Fortes Nordic A/S and their auditors regarding compliance with ISAE 3000 (the international standard for assurance engagements other than audits or reviews of historical financial information) and the General Data Protection Regulation (GDPR).

This document describes the technical and organizational measures implemented in connection with the operation of the SaaS solution Fortes Projectflow. It also provides information about the controls applied in the operation of Fortes Nordic and how they are implemented.

2.2 Projectflow Platform

Fortes Nordic A/S's processing activities consist of developing, operating, and distributing Projectflow as a "Software as a Service" (SaaS) solution, as well as providing related consulting services for implementation.

2.2.1 Fortes Nordic Description

Fortes Nordic A/S serves a wide range of clients across the Nordic region. Fortes Nordic supports Project and Portfolio Management (PPM), Resource Management, and Time Registration.

2.2.2 Basis for Processing

When delivering Fortes Nordic, Fortes Nordic A/S processes personal data as a data processor on behalf of the customer, who acts as the data controller. The processing is carried out in accordance with applicable laws and the data processing agreement concluded with the customer.

The customer is typically a self-governing/private institution, public authority, municipality, or private company. The data processing agreement and its appendices describe the services, types of personal data processed, and the data controller's instructions.

2.3 Nature of Processing

Fortes Nordic A/S's processing on behalf of the data controller primarily involves:

- Authentication of users
- Assignment and display of roles on projects, as well as immediate manager and department affiliation
- Track which users have created and updated information in the system over time.

The personal data processed is general (non-sensitive) personal data, including identification information such as:

- Name
- Picture
- Phone number
- Email address
- Department

For some customers, processing also includes time registration and absence registration (e.g., hours on holiday or sick leave).

2.4 Personal Data

Track which users have created and updated information in the system over time.

- Name and surname(s)
- Employee ID
- Email address
- Telephone number

- Workplace
- Time registrations

Categories of data subjects:

- Employees
- Partners/External collaborators

2.5 Practical Measures

Fortes Nordic A/S has established responsibility and organization for information security at the highest level, with the CEO and Head of Consulting & Operations jointly serving as the responsible security officers. They are tasked with preparing, implementing, and monitoring internal procedures and data protection policies, as well as conducting employee training.

Key measures include:

- Information security policy
- IT security manual
- IT security guidelines
- Information Security Forum (for high-level principal decisions)
- Change management
- Incident management
- Awareness training

Technical and organizational controls include, among others:

- Pseudonymization of personal data when indicated by the nature, scope, context, purpose, and risks of the processing
- Encryption of personal data based on risk assessment, with mandatory encryption for transmission of confidential/sensitive data over external links
- Annual risk assessments of processing systems and services, followed by appropriate technical and organizational mitigation measures
- Strict access control limited to authorized personnel with objective need, supported by regular access reviews and training
- Updated contingency plans, regular backups, and periodic testing of recovery procedures to ensure timely restoration after incidents
- Ongoing procedures for testing, assessing, and improving the effectiveness of all technical and organizational security measures
- Multi-factor authentication and secure encrypted connections for internet access to systems containing personal data
- Up-to-date encryption during data transmission and at rest, in line with current industry standards
- Physical security of processing locations, including protection against environmental hazards and unauthorized access
- Special handling of mobile storage media (encryption, logging, restricted access, secure disposal)
- Secure technical controls for home/remote working, including VPN, multi-factor authentication, and employee instructions
- Comprehensive logging of all personal data processing activities, with minimum six-month retention and verification
- Formal procedures for software updates, change management, separation of duties, and regular staff training on data protection
- Assistance to the data controller with data subject rights requests, breach notifications, risk assessments, and DPIAs
- Defined storage and deletion routines, with data returned or deleted upon termination as instructed
- Processing restricted to approved EU locations (currently Microsoft Azure in the Netherlands), with prior consent required for changes
- Appropriate safeguards for any transfers to third countries and procedures to handle and challenge third-country authority disclosure requests

2.6 Risk Assessment

Fortes Nordic A/S has assessed the potential consequences for data subjects in terms of confidentiality, integrity, and availability when processing personal data in connection with Fortes Nordic.

It is Fortes Nordic A/S's assessment that the processing presents a low risk to data subjects, given the nature of the data and the implemented security measures.

Fortes Nordic A/S conducts regular risk assessments, including:

- Identification and categorization of risks (likelihood and impact).
- Implementation of appropriate controls to mitigate risks.
- Support for Data Protection Impact Assessments (DPIAs) when required.

2.7 GDPR & Fortes Nordic A/S's Role and Responsibility as Data Processor

Fortes Nordic A/S acts as a data processor when delivering Fortes Nordic to the customer (the data controller). Fortes Nordic A/S supports the data controller in fulfilling its obligations regarding data subject rights.

Procedures and controls have been developed in the following main areas in accordance with the General Data Protection Regulation:

- Processing of personal data is carried out only in accordance with the instructions received under the data processing agreement.
- Appropriate technical measures have been implemented to ensure the security of processing.
- Appropriate organizational measures have been implemented to ensure the security of processing.
- Personal data can be deleted or returned upon termination of the agreement, as agreed with the data controller.
- Personal data is stored only for as long as agreed with the data controller.
- Only approved sub-processors are used, and Fortes Nordic A/S ensures adequate security through follow-up on their technical and organizational measures.
- Transfers of personal data to third countries or international organizations occur only in accordance with the agreement and on a valid transfer basis.
- Fortes Nordic A/S assists the data controller with handling data subject requests (e.g., access, rectification, erasure, or restriction of processing).
- Security incidents are handled in accordance with the terms of the data processing agreement.

Reference is also made to section 4, where the specific control activities are described.

Complementary controls at the data controllers

Certain controls are assumed to be implemented by the data controller and are essential for achieving the control objectives stated in this description. These include, among others, that the data controller:

- Ensures that personal data is kept up to date;
- Ensures that the instructions provided are lawful under the applicable data protection legislation at any given time;
- Ensures that the instructions are appropriate in relation to this data processing agreement and the main service agreement;
- Ensures that the controller's users and access rights are kept up to date.

3. Independent auditor's ISAE 3000 assurance report on the description of controls aimed at information security and processing of personal data

To the management of Fortes Nordic A/S and their customers

Scope

We were engaged to provide assurance about Fortes Nordic A/S' description in section 2 of Project and Portfolio Management for processing personal data in accordance with the data processing agreement with the data controllers as per May 4th 2026 ("the Description") and about the design of controls related to the control objectives stated in the Description.

We did not perform any procedures regarding the operating effectiveness of the controls included in the description, and, accordingly, do not express an opinion thereon.

We express reasonable assurance in our conclusion.

Fortes Nordic A/S uses Microsoft as a sub-processor for the hosting, web and services applied. The report uses the carve-out method and does not include control objectives and related controls performed by Microsoft.

Fortes Nordic A/S's responsibility

Fortes Nordic A/S is responsible for: preparing the Description and the accompanying statement in section 1, 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 requirements for independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, which is based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

Inforevision applies to the International Standard on Quality Management 1, ISQM 1, which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on Fortes Nordic A/S' description and on the design 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.

An assurance engagement to report on the Description and the design of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of its service and about the design 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. 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 and described in section 1.

As mentioned above, we did not perform any procedures regarding the operating effectiveness of the controls included in the description, and, accordingly, do not express an opinion thereon.

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 controller

Fortes Nordic 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 the service that the individual data controller 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.

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* in section 1. In our opinion, in all material respects:

- (a) The Description fairly presents the service designed and implemented as per May 4th 2026;
- (b) The controls related to the control objectives stated in the Description were appropriately designed as per May 4th 2026; and

Description of tests of controls

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

Intended users and purpose

This report and the description of tests of controls in section 4 are intended only for data controllers who have used Fortes Nordic A/S' service, 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.

Søborg, May 4th 2026

inforevision

statsautoriseret revisionsaktieselskab

John Richardt Søbjerg
State Authorized Public Accountant

Simon Okkels
Partner, Lead IT-auditor (CISA)

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

4.1 Objective and scope

Our work has been performed in accordance with ISAE 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information.

Our test of the design and implementation of the controls has included the control objectives and associated control activities selected by the management, which are stated in section 4.3. Any other control objectives, associated controls and controls at Fortes Nordic A/S customers are not covered by our tests.

This assurance report is prepared in accordance with the carve-out method and the description does not include control objectives and controls within Fortes Nordic A/S' subcontractors and sub-data processors.

4.2 Tests Performed

The tests performed to evaluate design and implementation of controls are mentioned below:

Method	Description overview
Enquiry	Enquiry with appropriate personnel at Fortes Nordic A/S has been conducted for all significant control activities. Enquiries have been made to obtain, among other things, knowledge and additional information about the policies and procedures implemented, including how the control activities are carried out. Furthermore, to get evidence of policies, procedures, and controls.
Inspection	Review and evaluation of policies, procedures and documentation that contain information on the performance of control activity. This includes reviewing and evaluating reports and other documentation to assess whether specific controls are designed so that they are expected to be effective if implemented. Furthermore, it is assessed whether controls are adequately monitored and controlled at appropriate intervals.
Observation	Observing how controls are performed.
Re-performing control procedures	The relevant control has been re-executed to verify that the control is functioning as expected

Control objective A (Instruction)

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.

No.	Fortes Nordic A/S's control activity	Auditors test activity	Result of auditors test
A1	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.	Checked by way of inspection that formalized procedures exist to ensure that personal data are only processed according to instructions. Checked by way of inspection that the procedures include a requirement to assess at least once a year the need for updates, including in case of changes in the data controller's instructions or changes in the data processing. Checked by way of inspection that procedures are up to date.	No deviations noted.
A2	The data processor only processes personal data stated in the instructions from the data controller.	Checked by way of inspection that Management ensures that personal data are only processed according to instructions. Checked by way of inspection of a sample of personal data processing operations that these are conducted consistently with instructions.	No deviations noted.
A3	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.	Checked by way of inspection that formalized procedures exist ensuring verification that personal data are not processed against the Regulation or other legislation. Checked by way of inspection that procedures are in place for informing the data controller of cases where the processing of personal data is evaluated to be against legislation.	No deviations noted.

Control objective B (Technical measures)

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	Fortes Nordic A/S's control activity	Auditors test activity	Result of auditors test
B1	Written procedures exist which include a requirement that safeguards agreed 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.	Checked by way of inspection that formalized procedures exist to ensure establishment of the safeguards agreed. Checked by way of inspection that procedures are up to date. Checked by way of inspection of a sample of data processing agreements that the safeguards agreed have been established.	No deviations noted.
B2	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 the safeguards agreed with the data controller.	Checked by way of inspection that formalized procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security. Checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data. Checked by way of inspection that the data processor has implemented the technical measures ensuring an appropriate level of security consistent with the risk assessment. Checked by way of inspection that the data processor has implemented the safeguards agreed with the data controller.	No deviations noted.
B3	For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.	Checked by way of inspection that, for the systems and databases used in the processing of personal data, antivirus software has been installed. Checked by way of inspection that antivirus software is up to date.	No deviations noted.
B4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	Checked by way of inspection that external access to systems and databases used in the processing of personal data takes place only through a secured firewall. Checked by way of inspection that the firewall has been configured in accordance with the relevant internal policy.	No deviations noted.

Control objective B (Technical measures)

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	Fortes Nordic A/S's control activity	Auditors test activity	Result of auditors test
B5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	Inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. Inspected network diagrams and other network documentation to ensure appropriate segmentation.	No deviations noted.
B6	Access to personal data is isolated to users with a work-related need for such access.	Checked by way of inspection that formalized procedures are in place for restricting users' access to personal data. Checked by way of inspection that formalized procedures are in place for following up on users' access to personal data being consistent with their work-related need. Checked by way of inspection that the technical measures agreed support retaining the restriction in users' work-related access to personal data. Checked by way of inspection of a sample of users' access to systems and databases that such access is restricted to the employees' work-related need.	No deviations noted.
B7	For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.	Checked by way of inspection that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.	No deviations noted.
B8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	Checked by way of inspection that formalized procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognised algorithm. Checked by way of inspection that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	No deviations noted.

Control objective B (Technical measures)

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	Fortes Nordic A/S's control activity	Auditors test activity	Result of auditors test
B9	Logging has been established in systems, databases and networks. For example: activities performed by administrators, security events such as changes in log settings, disabling logging, changes in user rights, failed login attempts. Logdata are protected against manipulation and technical errors and are reviewed regularly.	Checked by way of inspection that formalized procedures exist for setting up logging of user activities in systems, databases or networks that are used to process and transmit personal data, including review of and follow-up on logs. Checked by way of inspection that logging of user activities in systems, databases or networks that are used to process or transmit personal data has been configured and activated. Checked by way of inspection that user activity data collected in logs are protected against manipulation or deletion.	No deviations noted.
B10	Personal data used for development, testing or similar activity are always in pseudonymized or anonymized form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.	Checked by way of inspection that formalized procedures exist for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymized or anonymized form.	No deviations noted.
B11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	Checked by way of inspection that formalized procedures exist for regularly testing technical measures, including for performing vulnerability scans and penetration tests. Checked by way of inspection of samples that documentation exists regarding regular testing of the technical measures established.	No deviations noted.
B12	Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches.	Checked by way of inspection that formalized procedures exist for handling changes to systems, databases or networks, including handling of relevant updates, patches and security patches. Checked by way of inspection of extracts from technical security parameters and setups that systems, databases or networks have been updated using agreed changes and relevant updates, patches and security patches.	We have identified through sample testing that some devices are still running Windows 10, which is no longer being updated. These devices will therefore not receive future security or software updates and may consequently be exposed to known vulnerabilities. No further deviations noted.

Control objective B (Technical measures)

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	Fortes Nordic A/S's control activity	Auditors test activity	Result of auditors test
B13	A formalized procedure is in place for granting and removing users' access to personal data. Users' access is re-considered on a regular basis, including the continued justification of rights by a work-related need.	Checked by way of inspection that formalized procedures exist for granting and removing users' access to systems and databases using to process personal data. Checked by way of inspection of a sample of employees' access to systems and databases that the user accesses granted have been authorized and that a work-related need exists. Checked by way of inspection that documentation exists that user accesses granted are evaluated and authorized on a regular basis – and at least once a year.	No deviations noted.
B14	Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication.	Checked by way of inspection that formalized procedures exist to ensure that two-factor authentication is applied in the processing of personal data that involves a high risk for the data subjects. Checked by way of inspection that users' access to processing personal data that involve a high risk for the data subjects may only take place by using two-factor authentication.	No deviations noted.
B15	Physical access safeguards have been established so as to only permit physical access by authorized persons to premises and data centers at which personal data are stored and processed.	Checked by way of inspection that formalized procedures exist to ensure that only authorized persons can gain physical access to premises and data centers at which personal data are stored and processed. Checked by way of inspection of documentation that, throughout the assurance period, only authorized persons have had physical access to premises and data centers at which personal data are stored and processed.	No deviations noted.

Control objective C (Organisational measures)

Procedures and controls are complied with to ensure that the data processor has implemented organizational measures to safeguard relevant security of processing.

No.	Fortes Nordic A/S's control activity	Auditors test activity	Result of auditors test
C1	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 risk assessment performed. Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.	Checked by way of inspection that an information security policy exists that Management has considered and approved within the past year. Checked by way of inspection of documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No deviations noted.
C2	Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.	Inspected documentation of Management's assessment that the information security policy generally meets the requirements for safeguards and the security of processing in the data processing agreements entered into. Checked by way of inspection of a sample of data processing agreements that the requirements in these agreements are covered by the requirements of the information security policy for safeguards and security of processing.	No deviations noted.
C3	A check is carried out on the data processor's employees in connection with employment. The check includes, to the extent relevant: References from previous employment, criminal records, diplomas, etc.	Inspected that there are formalized procedures that ensure verification of the data processor's employees in connection with employment. Inspected via random sampling of data processor agreements, that the requirements for verification of employees in the agreements are covered by the data processor's verification procedures.	No deviations noted.
C4	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.	Inspected that formalized procedures are in place to ensure that employees, upon employment, sign a confidentiality agreement and are introduced to the information security policy and procedures relating to data processing.	No deviations noted.

Control objective C (Organisational measures)

Procedures and controls are complied with to ensure that the data processor has implemented organizational measures to safeguard relevant security of processing.

No.	Fortes Nordic A/S's control activity	Auditors test activity	Result of auditors test
C5	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.	Inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal and that assets such as access cards, computers, mobile phones, etc. are returned.	No deviations noted.
C6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed 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.	Checked by way of inspection that formalized procedures exist to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality.	No deviations noted.
C7	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.	Checked by way of inspection that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data. Inspected documentation that all employees who have either access to or process personal data have completed the awareness training provided.	No deviations noted.

Control objective D (Deletion and returning data)

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.

No.	Fortes Nordic A/S's control activity	Auditors test activity	Result of auditors test
D1	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.	Checked by way of inspection that formalized procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller. Checked by way of inspection that the procedures are up to date.	No deviations noted.
D2	The following specific requirements have been agreed for the data processor's retention periods and deletion routines: [insert description of concrete conditions]	Checked by way of inspection that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines. Checked by way of inspection of a sample of data processing sessions from the data processor's list of processing activities that documentation exists that personal data are stored in accordance with the agreed storage periods. Checked by way of inspection of a sample of data processing sessions from the data processor's list of processing activities that documentation exists that personal data are deleted in accordance with the agreed deletion routines.	No deviations noted.
D3	Upon termination of processing of personal data for the data controller, data is, in accordance with the agreement with the data controller: Returned to the data controller and/or deleted, where this does not conflict with other legislation.	Checked by way of inspection that formalized procedures are in place for processing the data controller's data upon termination of the processing of personal data.	No deviations noted.

Control objective E (Storing of personal data)

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.

No.	Fortes Nordic A/S's control activity	Auditors test activity	Result of auditors test
E1	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.	Checked by way of inspection that formalized procedures exist for only storing and processing personal data in accordance with the data processing agreements. Checked by way of inspection that the procedures are up to date. Checked by way of inspection of a sample of data processing sessions from the data processor's list of processing activities that documentation exists that data processing takes place in accordance with the data processing agreement.	No deviations noted.
E2	Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.	Checked by way of inspection that the data processor has a complete and updated list of processing activities stating localities, countries or regions. Checked by way of inspection of a sample of data processing sessions from the data processor's list of processing activities that documentation exists that the processing of data, including the storage of personal data, takes place only in the localities stated in the data processing agreement – or otherwise as approved by the data controller.	No deviations noted.

Control objective F (Sub-data-processors)

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.

No.	Fortes Nordic A/S's control activity	Auditors test activity	Result of auditors test
F1	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.	Checked by way of inspection that formalized procedures are in place for using sub-data processors, including requirements for sub-data processing agreements and instructions. Checked by way of inspection that procedures are up to date.	No deviations noted.
F2	The data processor only uses sub-data processors to process personal data that have been specifically or generally approved by the data controller.	Checked by way of inspection that the data processor has a complete and updated list of sub-data processors used. Checked by way of inspection of a sample of sub-data processors from the data processor's list of sub-data processors that documentation exists that the processing of data by the sub-data processor is stated in the data processing agreements – or otherwise as approved by the data controller.	No deviations noted.
F3	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.	Checked by way of inspection that formalized procedures are in place for informing the data controller when changing the sub-data processors used.	No deviations noted.
F4	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.	Checked by way of inspection for existence of signed sub-data processing agreements with sub-data processors used, which are stated on the data processor's list. Checked by way of inspection of a sample of sub-data processing agreements that they include the same requirements and obligations as are stipulated in the data processing agreements between the data controllers and the data processor.	No deviations noted.

Control objective F (Sub-data-processors)

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.

No.	Fortes Nordic A/S's control activity	Auditors test activity	Result of auditors test
F5	The data processor has an overview of approved sub-processors with an indication of: Name, CVR no., Address, description of the processing.	Checked by way of inspection that the data processor has a complete and updated list of sub-data processors used and approved. Checked by way of inspection that, as a minimum, the list includes the required details about each sub-data processor.	No deviations noted.
F6	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.	Checked by way of inspection that formalized procedures are in place for following up on processing activities at sub-data processors and compliance with the sub-data processing agreements. Checked by way of inspection of documentation that each sub-data processor and the current processing activity at such processor are subjected to risk assessment.	No deviations noted.

Control objective G (Transfer to third countries)

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.

No.	Fortes Nordic A/S's control activity	Auditors test activity	Result of auditors test
G1	Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organizations 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.	Checked by way of inspection that formalized procedures exist to ensure that personal data are only transferred to third countries or international organizations in accordance with the agreement with the data controller by using a valid basis of transfer. Checked by way of inspection that procedures are up to date.	We have been informed that for some customer solutions there are no agreements that the company may transfer data to third countries. No deviations noted.
G2	The data processor must only transfer personal data to third countries or international organizations according to instructions by the data controller.	Checked by way of inspection that the data processor has a complete and updated list of transfers of personal data to third countries or international organizations.	We have been informed that for some customer solutions there are no agreements that the company may transfer data to third countries. No deviations noted.
G3	As part of the transfer of personal data to third countries or international organizations, the data processor assessed and documented the existence of a valid basis of transfer.	Checked by way of inspection that formalized procedures are in place for ensuring a valid basis of transfer. Checked by way of inspection that procedures are up to date.	We have been informed that for some customer solutions there are no agreements that the company may transfer data to third countries. No deviations noted.

Control objective H (Data subject rights)

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.

No.	Fortes Nordic A/S's control activity	Auditors test activity	Result of auditors test
H1	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.	Checked by way of inspection that formalized procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects. Checked by way of inspection that procedures are up to date.	No deviations noted.
H2	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 detailed procedures for: Disclosure of information, Correction of information, Deletion of information, Limitation of processing of personal data, Information about processing of personal data to the data subject. Inspected documentation that the systems and databases used support the implementation of the detailed procedures mentioned.	No deviations noted.

Control objective I (Security breaches)

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.

No.	Fortes Nordic A/S's control activity	Auditors test activity	Result of auditors test
I1	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.	Checked by way of inspection that formalized procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. Checked by way of inspection that procedures are up to date.	No deviations noted.
I2	The data processor has established the following controls for the identification of possible breaches of personal data security: Awareness among employees, monitoring of network traffic, follow-up on logging of access to personal data.	Checked by way of inspection that the data processor provides awareness training to the employees in identifying any personal data breaches. Checked by way of inspection of documentation that network traffic is monitored and that anomalies, monitoring alarms, large file transfers, etc. are followed up on.	No deviations noted.
I3	If any personal data breach occurred, the data processor informed the data controller without undue delay and no later than 72 hours after having become aware of such personal data breach at the data processor or a sub-data processor.	Checked by way of inspection that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach.	No deviations noted.
I4	The data processor has established procedures for assistance to the data controller in the latter's notification to the Danish Data Protection Authority and takes into account the following important elements: The nature of the breach, probable consequences of the breach and measures taken or proposed to be taken to deal with the breach.	Inspected that the available procedures for notifying the data controllers in the event of a breach of personal data security contain detailed procedures for descriptions of: The nature of the breach, likely consequences of the breach and measures taken or proposed to be taken to deal with the breach. Inspected documentation that the existing procedures support that measures are taken to handle the breach of personal data security.	No deviations noted.

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."

Karsten Ley Poulsen

Managing Director

Serienummer: 431737e3-5f29-47a4-abca-65c168cc962d

IP: 87.48.xxx.xxx

2026-05-04 14:10:54 UTC



Simon Okkels

**inforevision statsautoriseret revisionsaktieselskab CVR:
19263096**

Partner, Lead IT-auditor (CISA)

Serienummer: 7ced0dfc-fff1-4f9c-a5b4-e6fcd672bf9a

IP: 93.165.xxx.xxx

2026-05-04 14:13:28 UTC



John Richardt Søbjærg

**inforevision statsautoriseret revisionsaktieselskab CVR:
19263096**

State Authorized Public Accountant

Serienummer: 70a986b1-9464-4830-8fb8-b43b6517911a

IP: 93.165.xxx.xxx

2026-05-04 14:16:19 UTC



Dette dokument er underskrevet digitalt via **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. 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.