

May 2026

CompuSoft A/S

ISAE 3000 ASSURANCE REPORT

CVR 21774774

Independent Auditor's ISAE 3000 assurance report on information security and data protection measures in relation to Data Processor Agreements with Data Controllers.



Structure of the Assurance Report

Chapter 1:

Management's statement.

Chapter 2:

Independent Auditor's Assurance Report.

Chapter 3:

Description of the control environment for the operation of CompuSoft A/S' data analysis services.

Chapter 4:

Auditor's description of control objectives, security measures, tests and findings.

Management's statement

CompuSoft A/S processes personal data on behalf of data controllers according to signed data processing agreements regarding data analysis services from CompuSoft A/S.

The data processing agreements currently cover a range of IT services, including hosting, booking and payment services, provided as a full-service supplier of intelligent booking and self-service solutions for campsites, holiday centres, sports centres, and other accommodation and tourism-related enterprises.

The accompanying description, Chapter 3, has been prepared for the use of customers, who have used the data analysis services from CompuSoft A/S, and who have sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves, when assessing, whether the demands to the control environment stated in data processing agreements, as well as requirements laid down in the General Data Protection Regulation are complied with.

CompuSoft A/S uses Cloudflare as a subservice organization/sub-processor. Cloudflare is a content delivery network (CDN) and cybersecurity company that provides website optimization, DDoS protection, and other security features to enhance the performance of the System and protect against online threats.

The assurance engagement applies the carve-out method and therefore does not include control objectives and related controls performed by Cloudflare on behalf of CompuSoft A/S.

Certain control objectives described in our system description in Section 3 can only be achieved if the complementary user entity controls are suitably designed and implemented in conjunction with our controls. The assurance engagement does not cover an evaluation of the suitability of the design of these complementary user entity controls.

CompuSoft A/S hereby confirms that:

- (A) The accompanying description, Chapter 3, gives a true and fair description of CompuSoft A/S' control environment in relation to data analysis services, which has processed personal data covered by the General Data Protection Regulation as of 22 January 2026. The criteria for this assertion are that the following description:
- (i) Gives an account of how the controls 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 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 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), communication, control activities, and monitoring controls that have been relevant to the processing of personal data.
- (ii) Includes relevant information about changes to the data processor's services for the processing of personal data implemented up to and including 22 January 2026.
- (iii) Does not omit or misrepresent information relevant for the scope of the controls described, taking into consideration that the description has been prepared to meet the common needs of a broad range of customers and their auditors, and may not, therefore, include every aspect of the control system that each individual customer may consider important in their own particular circumstances.
- (B) The controls related to the control objectives stated in the accompanying description were suitably designed as of 22 January 2026. The criteria for this assertion are that:
- (i) The risks threatening the fulfilment of the control objectives mentioned in the description were identified
 - (ii) The identified controls would, if used as described, provide reasonable assurance that the risks in question would not prevent the fulfilment of the said control objectives
- (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 General Data Protection Regulation.

Søndersø, 6 of May 2026

Kim Wolters
CEO, CompuSoft A/S

Independent auditor's ISAE 3000 assurance report on information security and data protection measures in relation to data processing agreements with CompuSoft A/S' customers

For CompuSoft A/S and relevant data controllers

Scope

We have been engaged to report on CompuSoft A/S' description of their services, see Chapter 3, in relation to data processing agreements with CompuSoft A/S' customers as of 22 January 2026 and on the design of controls regarding the control objectives stated in the description.

This assurance report covers whether CompuSoft A/S has designed appropriate controls related to the control objectives set out in Section 4. The assurance report does not include an assessment of CompuSoft A/S' overall compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, nor the Danish Act on Supplementary Provisions to the Regulation on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data (hereinafter referred to as the "data protection regulations").

CompuSoft A/S uses Cloudflare as a subservice organization/sub-processor. Cloudflare is a content delivery network (CDN) and cybersecurity company that provides website optimization, DDoS protection, and other security features to enhance the performance of the System and protect against online threats. The assurance engagement applies the carve-out method and therefore does not include control objectives and related controls performed by Cloudflare on behalf of CompuSoft A/S.

Certain control objectives described in CompuSoft A/S' system description in Section 3 can only be achieved if the complementary controls at the data controllers are suitably designed and implemented in conjunction with CompuSoft A/S' controls. The assurance engagement does not cover an evaluation of the suitability of the design of these complementary controls.

We express reasonable assurance in our conclusion.

CompuSoft A/S' responsibility

CompuSoft A/S is responsible for: preparing the description and the accompanying statements, 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 and implementing controls to achieve the stated control objectives.

Beierholm's independence and quality control

We have complied with the requirements of independence and other ethical requirements laid down in FSR's Ethical Rules based on fundamental principles of integrity, objectivity, professional competence and requisite care, confidentiality, and professional conduct.

We apply ISQM 1 and thus sustain a comprehensive system of quality management, including documented policies and procedures for compliance with ethical rules, professional standards as well as requirements in force under existing laws and additional regulation.

Auditor's responsibility

Our responsibility is to express an opinion, based on our procedures, on CompuSoft A/S' description and on the design and implementation of controls related to the control objectives stated in the said description.

We have conducted our engagement in accordance with ISAE 3000, Other assurance reports than audit or review of historical financial statements and additional requirements according to Danish audit regulation. The standard requires that we comply with ethical requirements and that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and whether the controls in all material aspects are appropriately designed.

An assurance engagement to report on the description, design, and implementation of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of their system, and about the design of controls. The procedures selected depend on the judgement of the data processor's auditor, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or implemented.

An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified and described by CompuSoft A/S in Chapter 3.

We have not performed procedures regarding the operating effectiveness of controls included in the description and express no opinion thereof.

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

Limitations of controls at CompuSoft A/S

CompuSoft A/S' description is prepared to meet the common needs of a broad range of customers and may not, therefore, include every aspect of the system that each individual customer may consider important in their own particular environment. Moreover, because of their nature, controls at CompuSoft A/S may not prevent or detect all breaches of personal data security.

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 CompuSoft A/S' services, such as this service was designed and implemented as of 22 January 2026; and
- b) The controls related to the control objectives stated in the description were suitably designed and implemented as of 22 January 2026.

Description of tests of controls

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



Intended users and purpose

This report and the description of the test of controls in Chapter 4 are solely intended for CompuSoft A/S' customers and their auditors, who have sufficient understanding to consider them along with other information, including information about the customers' own control measures, which the Data Controllers themselves have performed, when assessing whether the control environment is appropriate and there is compliance with the requirements of General Data Protection Regulations.

Copenhagen, 6 of May 2026.

Beierholm, Godkendt Revisionspartnerselskab, CVR 32 89 54 68

Kim Larsen

State-authorized Public Accountant

mne32179

Description of control environment for the operation of CompuSoft A/S' services.

Description of processing

The purposes of CompuSoft A/S' processing of personal data are to provide the data controllers' personnel with access to a system that enables them to manage customers' bookings and tickets and, in this connection, to collect payments and issue invoices, provide technical support, troubleshooting and maintenance of the System, and to protect against fraud, unlawful activities, and security breaches.

Introduction

CompuSoft A/S is a leading provider of booking systems and ticketing solutions for campsites, holiday centres, and tourism enterprises in Scandinavia. We offer omnichannel commerce solutions comprising e-commerce platforms, booking systems, guest applications, and access control. Our expertise in digitalisation and omnichannel strategy supports optimisation of business operations and guest services. We serve more than 600 campsites, holiday centres, and attractions on a daily basis.

Services and Applications Overview:

The processing performed by CompuSoft A/S primarily relates to the collection, recording, organisation, structuring, storage, adaptation, or alteration of personal data in accordance with the instructions of the data controllers.

Categories of Data Subjects Covered by the Data Processing Agreements

- Customers, prospective customers, and guests of the data controllers
- Employees of the data controllers (login information)

Types of Personal Data Processed

- **Customers, prospective customers, and guests:** Name, address, postal code, city, nationality, telephone number, card information, correspondence, content of free-text fields, purchased products, and email address. In addition, the period of stay, number of persons, age, and gender may be registered.
- **Employees:** Name, address, telephone number, and email address.

Special Categories of Personal Data

- **Civil registration number (CPR number):** May be processed in specific cases, and solely where the data controller is a municipal or governmental authority, and only to the extent necessary for the data controller in connection with the collection of payments.

Information Security Environment

The work with information security at CompuSoft A/S is based on generally accepted good practice for IT security and is inspired by the ISO 27001 standard, which applies a risk-based approach to information security management.

CompuSoft A/S has defined the following overall objectives for information security:

- The level of security shall be determined based on a risk-based approach balancing security considerations and compliance with data protection legislation against business considerations.
- Information security is managed in a professional and structured manner, inspired by the ISO/IEC 27001 standard as a framework for information security management and governance.
- All employees at CompuSoft A/S shall be aware that they play an important and active role in the company's overall information security. Employees are required to be familiar with and comply with applicable information security rules and guidelines relevant to their daily work and to participate in CompuSoft A/S' education and training activities within this area.

Practical Measures

CompuSoft A/S maintains a range of organisational and technical measures to safeguard the personal data processed under the data processing agreements. These measures include, but are not limited to:

- Ongoing vulnerability scanning
- Systematic patching and updating of software
- Monitoring of critical systems with notification in the event that systems do not operate as expected
- Network monitoring
- Logging of network activity
- Independent backup solutions
- Physical security and surveillance of data centres
- Redundant and independent emergency power supply systems
- Encryption
- Security incident management (incident and outage procedures)
- Segregation of user accounts and access rights

Control Measures

CompuSoft A/S further maintains a number of specific control measures designed to ensure that an appropriate level of security is maintained within the systems, including the following:

Employee instruction

Employees and any external collaborators are continuously informed of and receive adequate training and instruction regarding the purposes of processing, applicable policies, procedures, and their duty of confidentiality.

Access management and administration of user access

Only employees with a work-related need to process personal data are granted user access to the data controllers' personal data. Authorisations, including access rights, are revoked without undue delay when users no longer have a work-related need for access.

Control of failed access attempts

Based on a risk-based approach, failed access attempts are logged, and further attempts are blocked after a predefined number of consecutive failed attempts. Procedures are in place to ensure timely follow-up on failed access attempts where such follow-up is necessary to prevent personal data breaches and adverse effects for data subjects.

Change management

Formal change management procedures have been implemented to ensure that all changes are duly authorised, tested, and approved prior to implementation.

External communication connections

Technical measures have been implemented to protect systems and networks and to limit the risk of unauthorised access and/or installation of malicious code. Where required under applicable legislation, good data processing practice, or as otherwise covered by the master agreement, appropriate encryption technologies and equivalent measures are applied.

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

Complementary Controls at the Data Controllers

As part of the provision of the services, certain controls are assumed to be implemented by the data controllers and are essential to achieving the control objectives described in the system description.

The data controller has the following obligations:

- To continuously ensure that its own user access is kept up to date and that all users are aware of the access the system may provide to personal data
- To assess and test new versions of the solutions in connection with implementation (change management)
- To carry out GDPR clean-up routines to delete outdated or irrelevant personal data from the systems provided
- To stay informed by following newsletters and information bulletins issued by CompuSoft A/S
- To remain updated on CompuSoft A/S' operational information available via the CompuSoft Helpdesk Manager
- To assess whether the instruction is appropriate in relation to the entered data processing agreement

Auditor's description of control objectives, security measures, tests and findings

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
A.1	<p>Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures exist to ensure that personal data are only processed according to instructions.</p> <p>Checked by way of inspection that the procedures include a requirement to assess at least once a year the need for updates.</p> <p>Checked by way of inspection that procedures are up to date.</p>	<p>During our testing, we did not identify any deviations.</p>
A.2	<p>The data processor only processes personal data stated in the instructions from the data controller.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that Management ensures that personal data are only processed according to instructions.</p> <p>Checked by way of inspection of a sample of 1 personal data processing operations that these are conducted consistently with instructions.</p>	<p>During our testing, we did not identify any deviations.</p>

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
A.3	<p>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.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures exist ensuring verification that personal data are not processed against the Regulation or other legislation.</p> <p>Inquired if the data processor evaluates instructions from data processors with regards to the lawfulness of instructions.</p> <p>We have made inquiries as to whether management has ensured that current processing activities do not conflict with the General Data Protection Regulation or other applicable legislation</p>	<p>During our testing, we did not identify any deviations.</p>

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
B.1	<p>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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place to ensure that the agreed security measures are established.</p> <p>Checked by way of inspection that the procedures include a requirement to assess at least once a year the need for updates.</p> <p>Checked by way of inspection that the standard data processing agreement is in place and that the agreed security measures have been implemented.</p>	<p>During our testing, we did not identify any deviations.</p>
B.2	<p>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.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security.</p> <p>Checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data.</p> <p>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.</p> <p>Checked by way of inspection that the data processor has implemented the safeguards agreed with the data controller.</p>	<p>During our testing, we did not identify any deviations.</p>

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
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.	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that, for the systems and databases used in the processing of personal data, antivirus software has been installed.</p> <p>Checked by way of inspection that antivirus software is configured for automatic scanning of systems and databases.</p> <p>Checked by way of inspection that antivirus software is up to date.</p>	During our testing, we did not identify any deviations.
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>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.</p>	During our testing, we did not identify any deviations.
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inquiry whether internal networks are segmented to ensure restricted access to systems and databases used for processing personal data.</p> <p>Checked by way of inspection of network documentation that proper segmentation is in place.</p>	During our testing, we did not identify any deviations.

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
B.6	<p>Access to personal data is isolated to users with a work-related need for such access.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place for restricting users' access to personal data.</p> <p>Checked by way of inspection that formalised procedures are in place for following up to ensure that users' access to personal data is consistent with their work-related needs.</p>	<p>During our testing, we did not identify any deviations.</p>
B.7	<p>For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. This monitoring comprises:</p> <ul style="list-style-type: none"> • DISK usage • CPU usage • Anomalies, including attempts at unauthorised access • Memory errors • System errors 	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that system monitoring with alerting has been established for systems and databases used for processing personal data.</p> <p>Checked by way of inspection of a sample that proper follow-up on alerts is carried out.</p>	<p>During our testing, we did not identify any deviations.</p>
B.8	<p>Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place to ensure that transmission of sensitive and confidential information over the internet is protected by strong encryption based on a recognised algorithm.</p> <p>Checked by way of inspection that technological solutions for encryption have been available and activated as of the 22 January 2026.</p> <p>Checked by way of inspection that encryption is used for transmissions of sensitive and confidential personal data via the internet or by email.</p>	<p>During our testing, we did not identify any deviations.</p>

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
B.9	<p>Logging of the following matters has been established in systems, databases and networks:</p> <ul style="list-style-type: none"> • User logins • Execution of SQL commands • API server logging • User activity • File access • Security events comprising: <ul style="list-style-type: none"> ○ Changes to logging configurations, including disabling of logging ○ Changes to system permissions for users ○ Failed log-on attempts to systems, databases, and networks <p>Logon data are protected against manipulation and technical errors and are reviewed regularly.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place for configuring logging of user activities in systems, databases and networks used for processing and transmission of personal data, including review and follow-up on logs.</p> <p>Checked by way of inspection that logging of user activities in systems, databases and networks used for processing and transmission of personal data is configured and activated.</p> <p>Checked by way of inspection that collected information on user activity in logs is protected against manipulation and deletion.</p> <p>Checked by way of inspection of a sample of one day's logging that the log files contain the expected content according to the configuration and that there is documentation of the review and handling of any security incidents.</p> <p>Checked by way of inspection of a sample of one day's logging that there is documentation of the review of activities performed by system administrators and others with special privileges.</p>	<p>During our testing, we did not identify any deviations.</p>

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
B.10	Personal data must not be used for development, testing, or similar purposes.	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>We have made inquiries as to whether formalised procedures are in place for the use of personal data in test environments, ensuring that data is always anonymised or processed in accordance with valid instructions from the data controller.</p>	During our testing, we did not identify any deviations.
B.11	We have inspected that the established technical measures are continuously tested through vulnerability scans and penetration tests.	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that ongoing vulnerability scanning of systems and networks is performed.</p>	During our testing, we did not identify any deviations.
B.12	Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches.	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures exist for handling changes to systems, databases, or networks, including handling of relevant updates, patches, and security patches.</p> <p>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.</p>	During our testing, we did not identify any deviations.

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
B.13	<p>A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place for granting and revoking users' access to systems and databases used for processing personal data.</p> <p>Checked by way of inspection of a sample of an employee's access that the granted user access rights are approved and based on a work-related need.</p> <p>Checked by way of inspection that documentation exists for regular – at least annual – review and approval of granted user access rights.</p>	<p>During our testing, we did not identify any deviations.</p>
B.14	<p>Systems and databases processing personal data are accessed as a minimum by using two-factor authentication.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place to ensure that two-factor authentication is used when processing personal data that may pose a high risk to data subjects.</p> <p>Checked by way of observation that two-factor authentication is applied for external access to systems and databases.</p>	<p>During our testing, we did not identify any deviations.</p>

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
B.15	Physical access safeguards have been established to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed.	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place to ensure that only authorised persons can gain physical access to premises and data centres where personal data is stored and processed.</p> <p>Checked by way of inspection of documentation that only authorised persons had physical access to premises and data centres where personal data is stored and processed as at 22 January 2026.</p>	During our testing, we did not identify any deviations.

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
C.1	<p>The data processor's management 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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that an information security policy exists that Management has considered and approved within the past year.</p> <p>Checked by way of inspection of documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.</p>	<p>During our testing, we did not identify any deviations.</p>
C.2	<p>The data processor's management has ensured that the information security policy is not in conflict with the entered data processing agreements</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection of documentation that management has assessed that the information security policy generally meets the requirements for safeguards and processing security in the concluded data processing agreements.</p> <p>Checked by way of inspection of a sample data processing agreement that the requirements in the agreements are covered by the information security policy's requirements for safeguards and processing security.</p>	<p>During our testing, we did not identify any deviations.</p>

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
C.3	<p>The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant:</p> <ul style="list-style-type: none"> References from former employers. 	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place to ensure background checks of the data processor's employees in connection with recruitment.</p> <p>Checked by way of inspection, based on a sample of two newly hired employees, that documentation exists confirming that the background checks included:</p> <ul style="list-style-type: none"> References from previous employments (1) or an assessment of the necessity thereof (1) 	<p>During our testing, we did not identify any deviations.</p>
C.4	<p>Upon appointment, employees sign a confidentiality agreement.</p> <p>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.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place to ensure that employees sign confidentiality agreements upon employment and are introduced to the information security policy, procedures relating to the processing of personal data, and other relevant information.</p> <p>Checked by way of inspection, based on a sample of one newly hired employee, that a confidentiality agreement has been signed.</p> <p>Checked by way of inspection, based on a sample of one newly hired employee, that the employee has been introduced to the information security policy and procedures relating to the processing of personal data, as well as other relevant information.</p>	<p>During our testing, we did not identify any deviations.</p>

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
C.5	<p>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.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place to ensure that employees return their IT equipment upon termination of employment.</p> <p>Checked by way of inspection, based on a sample, that documentation exists confirming that the procedures were followed for the most recently terminated employee as at 22 January 2026.</p> <p>Checked by way of inspection, based on a sample, that the access rights of a terminated employee have been disabled or revoked.</p>	<p>During our testing, we did not identify any deviations.</p>
C.6	<p>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.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place to ensure that terminated employees are reminded of their ongoing obligations under confidentiality agreements and their general duty of confidentiality.</p> <p>Checked by way of inspection, based on a sample of one terminated employee, that documentation exists confirming continued adherence to the confidentiality agreement and the general duty of confidentiality.</p>	<p>During our testing, we did not identify any deviations.</p>

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
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.	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Inquired whether employees are continuously kept informed about IT security and relevant procedures.</p> <p>Checked by way of inspection that the data processor provides awareness training to employees covering general IT security and processing security in relation to personal data.</p>	During our testing, we did not identify any deviations.

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
D.1	<p>Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller.</p> <p>Checked by way of inspection that the procedures are up to date.</p>	<p>During our testing, we did not identify any deviations.</p>
D.2	<p>The following specific requirements have been agreed with respect to the data processor's storage periods and deletion routines:</p> <ul style="list-style-type: none"> Personal data may be retained for the full term of the agreement. 	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that the existing procedures for data retention and deletion include specific requirements relating to the data processor's retention periods and deletion routines.</p>	<p>During our testing, we did not identify any deviations.</p>
D.3	<p>Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been:</p> <ul style="list-style-type: none"> Returned to the data controller; and/or Deleted if this is not in conflict with other legislation 	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place for handling the data controller's data upon termination of personal data processing.</p> <p>Checked by way of inspection of a sample of a terminated processing activity that documentation exists showing that the agreed deletion or return of data has been carried out.</p>	<p>During our testing, we did not identify any deviations.</p>

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
E.1	<p>Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place to ensure that personal data is stored and processed solely in accordance with the data processing agreements.</p> <p>Checked by way of inspection that the procedures are up to date.</p> <p>Checked by way of inspection, based on a sample of one processing activity selected from the data processor's record of processing activities, that documentation exists confirming that the processing is carried out in accordance with the data processing agreement.</p>	<p>During our testing, we did not identify any deviations.</p>
E.2	<p>Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that the data processor maintains a complete and up-to-date record of processing activities indicating locations, countries or regions.</p> <p>Checked by way of inspection of a sample processing activity from the data processor's record of processing activities that documentation exists showing that the processing, including storage of personal data, is carried out only at the locations specified in the data processing agreement or otherwise approved by the data controller.</p>	<p>During our testing, we did not identify any deviations.</p>

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
F.1	<p>Written procedures exist which include requirements for the data processor when using sub-data processors, including requirements for sub-data processing agreements and instructions.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place for using sub-data processors, including requirements for sub-data processing agreements and instructions.</p> <p>Checked by way of inspection that procedures are up to date.</p>	<p>During our testing, we did not identify any deviations.</p>
F.2	<p>The data processor only uses sub-data processors to process personal data that have been specifically or generally approved by the data controller.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that the data processor maintains a complete and up-to-date overview of sub-processors used (1).</p> <p>Checked by way of inspection, based on one sub-processor selected from the data processor's overview of sub-processors, that documentation exists confirming that the sub-processor's processing activities are included in the data processing agreement or are otherwise approved by the data controller.</p>	<p>During our testing, we did not identify any deviations.</p>

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
F.3	<p>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.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place for notifying the data controller of changes in the use of sub-processors.</p> <p>Inquired of the data processor whether they can confirm that no changes have been made to the use of sub-processors as at 22 January 2026.</p>	<p>During our testing, we did not identify any deviations.</p>
F.4	<p>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.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that a signed sub-processor agreement exists with the subcontractor.</p> <p>Checked by way of inspection of a sample sub-processor agreement that it contains the same requirements and obligations as those stated in the data processing agreements between the data controllers and the data processor.</p>	<p>During our testing, we did not identify any deviations.</p>
F.5	<p>The data processor has a list of approved sub-data processors disclosing:</p> <ul style="list-style-type: none"> • Name; • Company identification • Address; • Description of the processing. 	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that the data processor maintains a complete and up-to-date record of used and approved sub-processors.</p> <p>Checked by way of inspection that the record contains at least the required information about each sub-processor.</p>	<p>During our testing, we did not identify any deviations.</p>

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
F.6	<p>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.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place for follow-up on processing activities performed by sub-processors and compliance with the sub-processing agreements.</p> <p>Checked by way of inspection of documentation that a risk assessment has been performed for each individual sub-processor and the relevant processing activities.</p> <p>Checked by way of inspection of documentation that appropriate follow-up has been conducted on the technical and organisational measures and processing security at the sub-processors used.</p>	<p>During our testing, we did not identify any deviations.</p>

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
G.1	<p>Written procedures exist which include a requirement that the data processor only transfers personal data to third countries or international organisations in accordance with the agreement with the data controller and on the basis of a valid transfer mechanism.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place to ensure that personal data is transferred to third countries or international organisations solely in accordance with the agreement with the data controller and on the basis of a valid transfer mechanism.</p> <p>Checked by way of inspection that the procedures are up to date.</p>	<p>During our testing, we did not identify any deviations.</p>
G.2	<p>The data processor is only permitted to transfer personal data to third countries or international organisations upon instruction from the data controller.</p>	<p>Checked by way of interview with relevant employees at CompuSoft A/S.</p> <p>Inquired of the data processor whether they can confirm that no assistance has been provided to data controllers in connection with transfers of data to third countries during the control period that did not follow instructions.</p> <p>Checked by way of inspection, based on a sample of one data processing agreement, that the agreement includes requirements that transfers of personal data to third countries may only be made upon specific instruction from the data controller.</p>	<p>During our testing, we did not identify any deviations.</p>

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
G.3	<p>The data processor has, in connection with transfers of personal data to third countries or international organisations, assessed and documented the existence of a valid transfer mechanism.</p>	<p>Checked by way of interview with relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place to ensure the establishment and maintenance of a valid transfer mechanism.</p> <p>Checked by way of inspection that the procedures are up to date.</p> <p>Checked by way of inspection that, for processing activities that may involve transfers to third countries, an assessment of the transfer mechanism has been performed, including the implementation of supplementary safeguards where relevant.</p> <p>Checked by way of inspection, based on a sample of one data transfer selected from the data processor's overview of transfers, that documentation exists confirming the existence of a valid transfer mechanism in the data processing agreement with the data controller, and that transfers have only taken place to the extent agreed with the data controller.</p>	<p>During our testing, we did not identify any deviations.</p>

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
H.1	<p>Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects.</p> <p>Checked by way of inspection that procedures are up to date.</p>	<p>During our testing, we noted that no written procedure exists containing a requirement that the data processor must assist the data controller in relation to data subjects' rights; however, this requirement is described in the data processing agreement template.</p>
H.2	<p>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.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>We have inspected that formalised procedures are in place for deletion and disclosure of personal data.</p> <p>We have made inquiries of the data processor as to whether they can confirm that, as at 22 January 2026, no requests for assistance have been received from data controllers in relation to disclosure, rectification, erasure, restriction of processing, or information to data subjects regarding the processing of personal data.</p>	<p>During our testing, we did not identify any deviations.</p>

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
I.1	<p>Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches.</p> <p>Checked by way of inspection that procedures are up to date.</p>	<p>During our testing, we did not identify any deviations.</p>
I.2	<p>The data processor has established the following controls to identify any personal data breaches:</p> <ul style="list-style-type: none"> • Awareness of employees; • Monitoring of network traffic; ness of employees; • Follow-up on logging of access to personal data 	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that the data processor provides awareness training to employees regarding the identification of potential personal data breaches.</p> <p>Checked by way of inspection that documentation exists confirming that network traffic is monitored and that anomalies, monitoring alerts, etc., are followed up appropriately.</p> <p>Checked by way of inspection that documentation exists confirming timely follow-up on logging of access to personal data, including repeated attempts to gain access.</p>	<p>During our testing, we did not identify any deviations.</p>

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.

No.	CompuSoft A/S' control activity	Auditor's test of controls	Test findings
I.3	<p>The data processor has, in the event of personal data breaches, notified the data controller without undue delay and no later than 12 hours after becoming aware of a personal data breach at the data processor or a sub-processor.</p>	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of interview with relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that the data processor maintains an overview of security incidents, indicating whether each individual incident constituted a personal data breach.</p> <p>Inquired of the data processor whether they can confirm that no personal data breaches have been identified at sub-processors as at 22 January 2026.</p>	<p>During our testing, we did not identify any deviations.</p>
I.4	<p>The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency:</p> <ul style="list-style-type: none"> • Nature of the personal data breach; • Probable consequences of the personal data breach; • Measures taken or proposed to be taken to respond to the personal data breach. 	<p>We have interviewed relevant employees at CompuSoft A/S.</p> <p>Checked by way of inspection that the procedures in place for informing the data controllers in the event of any personal data breach include detailed procedures for:</p> <ul style="list-style-type: none"> • Describing the nature of the personal data breach; • Describing the probable consequences of the personal data breach; • Describing measures taken or proposed to be taken to respond to the personal data breach. <p>Checked by way of inspection of documentation, that the procedures available, support that measures are taken to respond to the personal data breach.</p>	<p>During our testing, we did not identify any deviations.</p>

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."

Kim Holm Larsen

Beierholm Godkendt Revisionspartnerselskab CVR: 32895468

Statsautoriseret revisor / State-authorized Public Accountant

På vegne af: Beierholm Godkendt Revisionspartnersels...

Serienummer: bff7239f-6800-4339-865f-dbc13a357020

IP: 212.98.xxx.xxx

2026-05-06 13:48:39 UTC



Kim Røtticher Wolters

CEO

På vegne af: CompuSoft A/S

Serienummer: d9f7ae18-ce37-4e7a-a582-af6337270608

IP: 212.98.xxx.xxx

2026-05-11 07:04:13 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.