Compaya A/S

Palægade 4, 2. tv.
1261 København K
CVR.NR. 31 37 54 28

ISAE 3000, type 2

Independent auditor's ISAE 3000 assurance report on the description of controls aimed at information security and processing of personal data throughout the period from 1st June 2025 to 31st May 2026

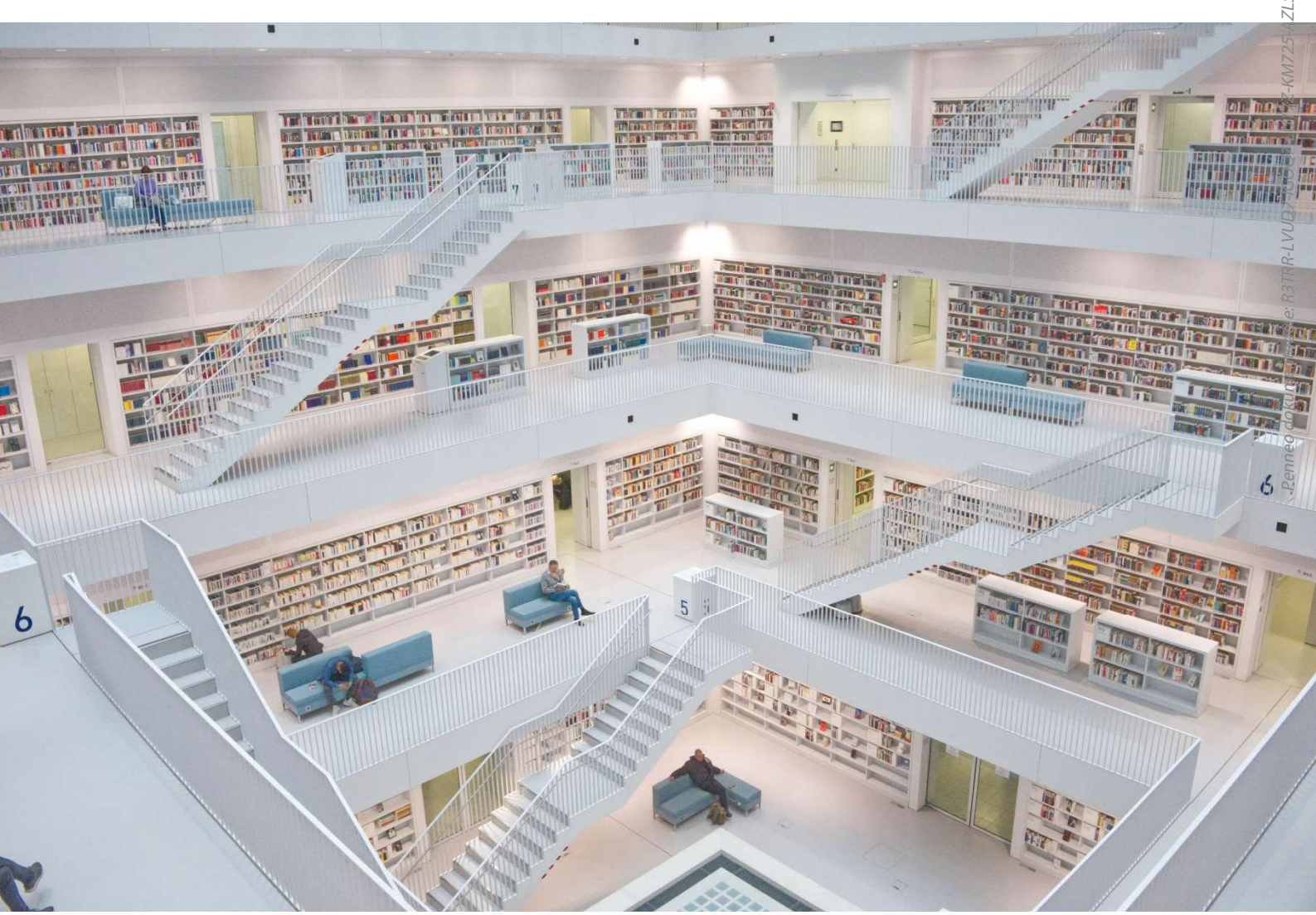

Table of Contents

S.nr. 302391

AOG/JR

1. Management's statement

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

The accompanying description has been prepared for the data controllers, who use Compaya A/S' SMS-systems, and who have 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.

Compaya A/S uses team.blue Denmark A/S and Rackhosting ApS as sub-processors for hosting and network services. The assurance report applies the carve-out method and does not include the control objectives and related controls performed by team.blue Denmark A/S and Rackhosting ApS on behalf of Compaya A/S.

Certain control objectives included in the description in Section 2 can only be achieved if the complementary controls at Compaya A/S' customers are suitably designed and operate effectively in conjunction with our controls. The assurance report does not cover the suitability of the design or the operating effectiveness of these complementary controls.

Compaya A/S confirms, that:

a) The accompanying description, in section 2, provides an accurate description of SMS-systems services, that processes personal data for data controllers covered by the Regulation throughout the period from 1st June 2025 to 31st May 2026. The criteria used in making this statement were that the accompanying description:

   (i) Presents how Compaya 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, 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) and communication, control activities and monitoring controls that are relevant to the processing of personal data;

(ii) Includes relevant information about changes in the processing of personal data in the period from 1st June 2025 to 31st May 2026.

(iii) 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 operated effectively throughout the period from 1st June 2025 to 31st May 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

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1st June 2025 to 31st May 2026.

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.

Copenhagen, 25th August 2026
Compaya A/S

Martin Saldorn Schrøder
CEO

2. COMPAYA A/S' DESCRIPTION OF THE SMS SYSTEMS

COMPAYA A/S
Compaya A/S (Compaya) is a Danish-owned company that develops and operates the online services CPSMS.dk, ProSMS.se/SMS.dk and SMS1919 for businesses, associations, public institutions, etc. Compaya has an office in Copenhagen.

Compaya's approximately eight employees specialize in sales and marketing, system development, server operations, support and information security, and are organized into a Sales Department and a Development Department.

The IT Security Officer manages Compaya's personal data security in relation to the processing carried out by Compaya on behalf of its customers, including entering into data processing agreements, responding to enquiries from data controllers, notification of personal data breaches, compliance with internal policies and procedures, and similar matters.

THE SMS SYSTEMS AND PROCESSING OF PERSONAL DATA
Compaya provides the SMS systems as Software-as-a-Service (SaaS) solutions. In order to use the SMS systems, customers must accept the terms and conditions available on the respective systems' websites. In some cases, customers request a specific master agreement, in which case such an agreement is prepared upon request. Through the websites and the SMS systems, we encourage customers to enter into a data processing agreement. This is either generated electronically or, where required, Compaya's standard data processing agreement, adapted to the individual customer, is provided.

The SMS systems are developed at the Copenhagen office but are operated from external hosting centres, which therefore act as sub-processors. Compaya has entered into data processing agreements with these sub-processors. In connection with the data controller's use of the SMS systems, Compaya collects and processes personal data relating to the data controller. Such data includes company name, address, name, email address, telephone number, CVR number and, where applicable, EAN number, as well as activity logs relating to the use of the SMS systems. The data consists solely of ordinary, non-sensitive personal data.

In the SMS systems, the data controller's users enter personal data concerning recipients of SMS messages. Specifically, this consists of mobile telephone numbers and, where applicable, names. Data controllers may also enter personal data in the text field of the SMS message itself.

As a general rule, Compaya processes data by storing and transmitting the SMS messages entered into the SMS systems by the data controllers. A log of sent SMS messages is retained, and Compaya employees have access, via this log, to the information contained in the SMS messages through the user roles configured as system access rights. Such access is used when resolving problems on behalf of data controllers.

PERSONAL DATA SECURITY MANAGEMENT
Compaya has established requirements for the establishment, implementation, maintenance and continuous improvement of a personal data security management system designed to ensure compliance with agreements entered into with data controllers, good data processing practices and relevant requirements applicable to data processors pursuant to the General Data Protection Regulation (GDPR) and the Danish Data Protection Act.

The technical and organizational security measures and other controls for the protection of personal data have been designed on the basis of risk assessments and are implemented to ensure confidentiality, integrity and availability, as well as compliance with applicable data protection legislation. To the greatest extent possible, security measures and controls are automated and technically supported by IT systems.

The management of personal data security, as well as the technical and organizational security measures and other controls, is structured into the following principal areas, for which control objectives and control activities have been defined:

ARTICLE	AREA
Article 28(1)	Guarantees provided by the processor
Article 28(3)	Data processing agreement
Article 28(3)(a) and (h), and Article 28(10), Article 29, Article 32(4)	Instructions for the processing of personal data
Article 28(2) and (4)	Sub-processors
Article 28(3)(b)	Confidentiality and statutory duty of confidentiality
Article 28(3)(c)	Technical and organizational security measures
Article 25	Data protection by design and by default
Article 28(3)(g)	Deletion and return of personal data
Article 28(3)(e), (f) and (h)	Assistance to the data controller
Article 30(2), (3) and (4)	Record of categories of processing activities
Article 33(2)	Notification of personal data breaches

RISK ASSESSMENT

Management is responsible for ensuring that all measures necessary to address the threat landscape faced by Compaya at any given time are initiated, so that the implemented security measures and controls remain appropriate and the risk of personal data breaches is reduced to an appropriate level.

An ongoing assessment is performed to determine the appropriate level of security. The assessment takes into account risks relating to the accidental or unlawful destruction, loss or alteration of personal data, or unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.

As a basis for updating the technical and organizational security measures and other controls, a risk assessment is performed once a year. The risk assessment evaluates the likelihood and consequences of events that may threaten personal data security and, consequently, the rights and freedoms of natural persons, including accidental, deliberate and unintentional events.

The risk assessment takes into account the state of the art and the costs of implementation. As part of the risk assessment, a Data Protection Impact Assessment (DPIA) has been performed for the SMS systems. Compaya has also used the Risknon model from Risikoanalyser.dk for its risk analysis.

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES AND OTHER CONTROLS

The technical and organizational security measures and other controls relate to all processes and systems that process personal data on behalf of the data controller. The control objectives and control activities specified in the control schedule form an integral part of the description below.

Guarantees Provided by the Processor

Compaya has implemented policies and procedures to ensure that Compaya is able to provide sufficient guarantees that appropriate technical and organizational security measures are implemented in such a manner that processing meets the requirements of the GDPR and ensures the protection of the rights of data subjects.

Compaya has established an organizational structure for personal data security and has prepared and implemented an information security policy approved by management, which is regularly reviewed and updated.

Procedures are in place for the recruitment and termination of employees, as well as guidelines for the training and instruction of employees who process personal data, including the implementation of awareness and information campaigns.

Data Processing Agreements
Compaya has implemented a procedure for entering into data processing agreements specifying the conditions for processing personal data on behalf of the data controller. Compaya uses the Danish Data Protection Agency's template for data processing agreements in accordance with the services provided, including information concerning the use of sub-processors. The data processing agreements are signed by both parties and stored electronically.

As a processor, Compaya only processes personal data on documented instructions from the data controller, either in the data processing agreement or, in some cases, pursuant to separate instructions prepared by the data controller.

As a processor, Compaya immediately informs the data controller if, in Compaya's opinion, an instruction infringes the GDPR or other data protection provisions under EU law or the national law of Member States.

Sub-processors
The processor has the data controller's general authorization to use sub-processors. However, the processor must obtain the data controller's approval of any intended changes concerning the addition or replacement of sub-processors, thereby giving the data controller the opportunity to object to such changes.

Compaya only uses sub-processors for server hosting in connection with the operation of the SMS systems.

Each year, typically in March, the sub-processor must provide an assurance report for the preceding year issued by an approved audit firm concerning the sub-processor's implementation of its own guidelines and the adequacy thereof.

Confidentiality and Statutory Duty of Confidentiality
As a processor, Compaya ensures that only persons currently authorized to do so have access to personal data processed on behalf of the data controller. Access to the data is therefore revoked immediately if the authorization is withdrawn or expires.

Only persons for whom access to the personal data is necessary in order to fulfil the processor's obligations towards the data controller may be authorized.

As a processor, Compaya ensures that persons authorized to process personal data on behalf of the data controller have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality.

At the request of the data controller, Compaya can demonstrate that the relevant employees are subject to the aforementioned duty of confidentiality.

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES
Risk Assessment
Compaya has implemented the technical and organizational security measures on the basis of an assessment of risks relating to confidentiality, integrity and availability. Reference is made to the separate section concerning this matter.

Contingency Plans
Compaya has established contingency plans to ensure that the availability of and access to personal data can be restored in a timely manner in the event of physical or technical incidents. Compaya has established an emergency response organization that is activated in such cases. An emergency response team has been established, and guidelines for activating the emergency response organization have been implemented.

Compaya has prepared detailed contingency plans and plans for the restoration of systems and data. The plans are available via Dropbox. They are tested and revised on an ongoing basis in connection with changes to systems, etc.

Storage of Personal Data
Compaya has implemented procedures to ensure that personal data is stored only in accordance with Compaya's personal data policy. Access to personal data is granted on the basis of work-related needs and the need-to-know principle.

Physical Access Control

Compaya has implemented procedures to ensure that its premises are protected against unauthorized access. Compaya does not have secured areas such as server rooms and therefore does not use key-card access control or similar measures. Customers, suppliers and other visitors are accompanied while on the premises. Outside normal working hours, an alarm system code is required to gain access to the premises.

Compaya uses hosting providers for all servers. Compaya does not have access to the hosting providers' facilities. Only authorized employees of the hosting providers have access to these facilities.

Logical Access Security

Compaya has established controls to ensure that access to systems and data is protected against unauthorized access to personal data. Users are created with a unique user ID and password, and the user ID is used when granting access to resources and systems.

All system access rights are granted on the basis of work-related needs. At least once a year, users' continued work-related need for access is evaluated, including the validity and correctness of assigned user rights. Procedures and controls support the processes for creating, modifying and deleting users, assigning access rights and reviewing such rights.

Requirements concerning, among other things, password length and complexity, as well as account lockout following unsuccessful login attempts, follow best practices for secure logical access control. Technical measures have been designed to support these requirements.

Remote Workstations and Remote Access to Systems and Data

Compaya has implemented procedures to ensure that access from workplaces outside Compaya's premises and remote access to servers and data take place via VPN connections. Compaya has implemented procedures to ensure that external communication connections are secured by encryption.

Network Security

Compaya has implemented procedures to ensure appropriate network use and security. Compaya's operational networks are hosted by team.blue Denmark A/S (Zitcom/Curanet/Wannafind) and Rackhosting ApS and are separated from Compaya's office network. Access between the networks is restricted as far as possible and is managed as described above.

At Compaya's premises in Palægade, only network equipment relating to the office network is located. The office network is divided into VLANs.

Compaya's office network at Palægade 4 is protected by the firewall in its router, which generally blocks all incoming traffic and permits all outgoing traffic. All PCs and laptops are additionally protected by the software firewall included in Bitdefender Endpoint Security.

The CPSMS and SMS1919 systems are hosted by team.blue and are protected by the firewall operated by team.blue. The PROSMS system is hosted by Rackhosting and is protected by the hardware firewall operated by Rackhosting. Each server is also protected by a software firewall administered by Compaya.

Antivirus Software and System Updates

Compaya has implemented procedures to ensure that devices with access to networks and applications are protected against viruses and malware. Antivirus software and other protection systems are continuously updated and adapted to the current threat level.

Compaya has implemented procedures to ensure that system software is continuously updated in accordance with suppliers' instructions and recommendations. Patch Management procedures cover operating systems, critical services and relevant software installed on servers and workstations.

Backup and Restoration of Data

Compaya has implemented procedures to ensure that systems and data are backed up in order to mitigate data loss or loss of availability in the event of a system failure. Backups are stored at an alternative location. Restore testing of backups is performed on an ongoing basis and at least once a year.

Logging of the Use of Personal Data
Compaya has implemented procedures to ensure that logging is configured in accordance with statutory requirements and business needs, based on a risk assessment of the systems and the current threat level.

The scope and quality of log data are sufficient to identify and demonstrate potential misuse of systems or data, and log data is regularly reviewed for usability and abnormal behaviour. Log data is protected.

Monitoring
Compaya has implemented procedures to ensure continuous monitoring of systems and implemented technical security measures.

Disposal of IT Equipment
Storage media that are to be destroyed may be handed over to the IT Security Officer or the Head of IT Development, who is responsible for ensuring effective and permanent destruction of the media or the data contained on them.

DATA PROTECTION BY DESIGN AND BY DEFAULT
Compaya has implemented policies and procedures for the development and maintenance of the SMS systems to ensure a controlled change process. A Change Management procedure is used to manage development and change tasks, and each task follows a consistent process.

Development, test and production environments are separated, and every development and change task undergoes a testing process. Procedures have been implemented for version control, logging and backup, making it possible to reinstall previous versions.

DELETION AND RETURN OF PERSONAL DATA
Compaya has implemented policies and procedures to ensure that personal data is deleted in accordance with instructions from the data controller when the processing of personal data ceases upon expiry of the contract with the data controller.

ASSISTANCE TO THE DATA CONTROLLER
Compaya has implemented policies and procedures to ensure that Compaya can assist the data controller in fulfilling its obligation to respond to requests concerning the exercise of data subjects' rights.

Compaya has implemented policies and procedures to ensure that Compaya can assist the data controller in ensuring compliance with the obligations under Article 32 concerning security of processing, Article 33 concerning notification and communication of personal data breaches, and Articles 34–36 concerning data protection impact assessments and related obligations.

Compaya has implemented policies and procedures to ensure that Compaya can make available to the data controller all information necessary to demonstrate compliance with the requirements applicable to processors.

Compaya also allows for and contributes to audits, including inspections, conducted by the data controller or another auditor authorized by the data controller.

RECORD OF CATEGORIES OF PROCESSING ACTIVITIES
Compaya has implemented policies and procedures to ensure that a record is maintained of the categories of processing activities carried out on behalf of the data controller. The record is updated regularly and reviewed as part of the annual review of policies and procedures, etc.

The record is stored electronically and can be made available to the supervisory authority upon request.

NOTIFICATION OF PERSONAL DATA BREACHES
Compaya has implemented policies and procedures to ensure that personal data breaches are recorded with detailed information concerning the incident and that the data controller is notified without undue delay after Compaya becomes aware that a personal data breach has occurred.

The recorded information enables the data controller to assess whether the personal data breach must be reported to the supervisory authority and whether the data subjects must be notified.

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 specified in the description.
The data controller has, among other things, the following obligations:

- Ensuring that the instructions contained in the data processing agreement entered into are lawful under the data protection legislation applicable from time to time.
- Ensuring that the instructions contained in the data processing agreement are appropriate in relation to the principal service.
- Responsibility for ensuring that administrators' use of the SMS systems and the processing of personal data performed in the systems comply with data protection legislation.
- Ensuring that any specific requirements relating to security measures at the data controller are described in the data processing agreement entered into.
- Ensuring that the data controller's users in the SMS systems are kept up to date.

CHANGES DURING THE REPORTING PERIOD

During the reporting period, Compaya changed auditors, and consequently the structure of the assurance report may differ slightly from previous reports.

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 Compaya A/S and their customers

Scope
We were engaged to provide assurance about Compaya A/S' description in section 2 for processing personal data in accordance with the data processing agreement with the data controllers throughout the period 1st June 2025 to 31st May 2026 ("the Description") and about the design and operating effectiveness of controls related to the control objectives stated in the Description.

We express reasonable assurance in our conclusion.

Compaya A/S uses team.blue Denmark A/S and Rackhosting ApS as sub-processors for hosting and network services. The assurance report applies the carve-out method and does not include the control objectives and related controls performed by team.blue Denmark A/S and Rackhosting ApS on behalf of Compaya A/S.

Certain control objectives included in the description in Section 2 can only be achieved if the complementary controls at Compaya A/S' customers are suitably designed and operate effectively in conjunction with our controls. The assurance report does not cover the suitability of the design or the operating effectiveness of these complementary controls.

Compaya A/S' responsibility
Compaya 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 Compaya A/S' description and on the design and operating effectiveness of controls related to the control objectives stated in that Description, based on our procedures.

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

An assurance engagement to report on the Description, design, and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of its service and about the design and operating effectiveness of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not appropriately designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data processor and described in section 1.

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
Compaya 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. Furthermore, the projection of any evaluation of the operating effectiveness to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion
Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the *Management's statement* in section 1. In our opinion, in all material respects:

(a) The Description fairly presents the service designed and implemented throughout the period 1st June 2025 to 31st May 2026;

(b) The controls related to the control objectives stated in the Description were appropriately designed throughout the period 1st June 2025 to 31st May 2026; and

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period 1st June 2025 to 31st May 2026.

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 Compaya 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, 25th August 2026

inforevision
statsautoriseret revisionsaktieselskab

John Richardt Søbjærg
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 Compaya 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 Compaya 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 Compaya 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

4.3 Control objectives, Controls and Test results

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.	Compaya'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 formalised 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 formalised 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. Checked by way of inspection that the data controller was informed in cases where the processing of personal data was evaluated to be against legislation.	We have been informed that there were no instances during the period in which the company assessed the instructions to be in violation of applicable 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.	Compaya'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 formalised 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 formalised 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.	Compaya'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 formalised procedures are in place for restricting users' access to personal data. Checked by way of inspection that formalised 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. Checked by way of inspection that, in a sample of alarms, these were followed up on and that the data controllers were informed thereof as appropriate.	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.	Compaya's control activity	Auditors test activity	Result of auditors test
B8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	Checked by way of inspection that formalised 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 technological encryption solutions have been available and active throughout the assurance period. 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.
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. Log data are protected against manipulation and technical errors and are reviewed regularly.	Checked by way of inspection that formalised 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. Checked by way of inspection of a sample of days of logging that the content of log files is as expected compared to the setup and that documentation exists regarding the follow-up performed and the response to any security incidents. Checked by way of inspection of a sample of days of logging that documentation exists regarding the follow-up performed for activities carried out by system administrators and others holding special rights.	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.	Compaya's control activity	Auditors test activity	Result of auditors test
B10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.	Checked by way of inspection that formalised procedures exist for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised form. Checked by way of inspection of a sample of development or test databases that personal data included therein are pseudonymised or anonymised.	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 formalised 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. Checked by way of inspection that any deviations or weaknesses in the technical measures have been responded to in a timely and satisfactory manner and communicated to the data controllers as appropriate.	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 formalised 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.	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.	Compaya's control activity	Auditors test activity	Result of auditors test
B13	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.	Checked by way of inspection that formalised 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 authorised and that a work-related need exists. Checked by way of inspection of a sample of resigned or dismissed employees that their access to systems and databases was deactivated or removed on a timely basis. Checked by way of inspection that documentation exists that user accesses granted are evaluated and authorised on a regular basis – and at least once a year.	We have identified that the process for deactivating access for one terminated employee, as well as the subsequent user access review, did not operate effectively during the period, as access to one system used for internal communication was not deactivated in a timely manner. No further 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 formalised 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 authorised persons to premises and data centres at which personal data are stored and processed.	Checked by way of inspection that formalised procedures exist to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed. Checked by way of inspection of documentation that, throughout the assurance period, only authorised persons have had physical access to premises and data centres 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 organisational measures to safeguard relevant security of processing.			
No.	Compaya'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. Inspected via a random sample of newly employed employees during the declaration period, that there is documentation that the verification has included references from previous employment, criminal records, diplomas, etc., to the relevant extent.	We have been informed that there were no new hires during the period. It was therefore not possible to test the effectiveness of the control. No deviations noted.

Control objective C (Organisational measures) Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.			
No.	Compaya's control activity	Auditors test activity	Result of auditors test
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 by a sample of newly hired employees during the declaration period, that the employees in question have signed a confidentiality agreement. Inspected by a sample of newly hired employees during the declaration period, that the employees in question have been introduced to: the information security policy, procedures regarding data processing, as well as other relevant information.	We have been informed that there were no new hires during the period. It was therefore not possible to test the effectiveness of the control. No deviations noted.
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. Checked by way of inspection of employees resigned or dismissed during the assurance period that rights have been deactivated or terminated and that assets have been returned.	We have identified that the process for deactivating access for one terminated employee did not operate effectively during the period. No further 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 formalised 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. Checked by way of inspection of employees resigned or dismissed during the assurance period that documentation exists 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.	Compaya'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 formalised 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.	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 formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data. Checked by way of inspection of terminated data processing sessions during the assurance period that documentation exists that the agreed deletion or return of data has taken place.	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.	Compaya'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 formalised 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.	Compaya'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 formalised 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 formalised procedures are in place for informing the data controller when changing the sub-data processors used. Inspected documentation that the data controller was informed when changing the sub-data processors used throughout the assurance period.	We have been informed that there were no changes to the sub-processors during the period, and we have therefore been unable to test the effectiveness of the control. 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.	Compaya'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 formalised 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. Checked by way of inspection of documentation that technical and organisational measures, security of processing at the sub-data processors used, third countries' bases of transfer and similar matters are appropriately followed up on.	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.	Compaya'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 organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures exist to ensure that personal data are only transferred to third countries or international organisations 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 none of the customer solutions, there are agreements permitting the company to transfer data to third countries. No deviations noted.
G2	The data processor must only transfer personal data to third countries or international organisations 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 organisations. Checked by way of inspection of a sample of data transfers from the data processor's list of transfers that documentation exists that such transfers were arranged with the data controller in the data processing agreement or subsequently approved.	We have been informed that, for none of the customer solutions, there are agreements permitting the company to transfer data to third countries. No deviations noted.
G3	As part of the transfer of personal data to third countries or international organisations, the data processor assessed and documented the existence of a valid basis of transfer.	Checked by way of inspection that formalised procedures are in place for ensuring a valid basis of transfer. Checked by way of inspection that procedures are up to date. Checked by way of inspection of a sample of data transfers from the data processor's list of transfers that documentation exists of a valid basis of transfer in the data processing agreement with the data controller and that transfers have only taken place in so far as this was arranged with the data controller.	We have been informed that, for none of the customer solutions, there are agreements permitting the company to 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.	Compaya'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 formalised 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. Inspected that documentation for requests for assistance from the data controller in relation to the provision, correction, deletion or restriction of and information on the processing of personal data to the data subject has been completed correctly and in a timely manner.	We have been informed that no assistance was provided to the data controller during the period, and we have therefore been unable to test the effectiveness of the control. 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.	Compaya'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 formalised 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. Checked by way of inspection of documentation that logging of access to personal data, including follow-up on repeated attempts to gain access, is followed up on, on a timely basis.	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. Made inquiries of the sub-data processors as to whether they have identified any personal data breaches throughout the assurance period. Checked by way of inspection that the data processor has included any personal data breaches at sub-data processors in the data processor's list of security incidents. Checked by way of inspection that all personal data breaches recorded at the data processor or the sub-data processors have been communicated to the data controllers concerned without undue delay and no later than 72 hours after the data	We have been informed that there were no personal data breaches during the reporting period. 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.	Compaya's control activity	Auditors test activity	Result of auditors test
		processor became aware of the personal data breach.	
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. Inspected documentation that, in the event of a breach of personal data security, measures have been taken to deal with the breach of personal data security.	No deviations noted.

5. Managements comments on Result of Auditors test

Compaya A/S has the following statement regarding the outcome of the assurance report:

No.	*Compaya's control activity*	*Auditors test activity*	*Management's response*
B13	A formalized 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.	We have identified that the process for deactivating access for one terminated employee, as well as the subsequent user access review, did not operate effectively during the period, as access to one system used for internal communication was not deactivated in a timely manner.	This concerns the Slack system, which is used solely for internal communication.
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.	We have identified that the process for deactivating access for one terminated employee did not operate effectively during the period.	This concerns the Slack system, which is used solely for internal communication.

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."

Martin Saldern Schrøder
Direktør
Serienummer: e227fbdb-8ee7-42c5-94e0-69223948aaf3
IP: 152.115.xxx.xxx
2026-08-25 08:32:17 UTC

Mit ID

Simon Okkels
inforevision statsautoriseret revisionsaktieselskab CVR: 19263096
Partner, Lead IT-auditor (CISA)
Serienummer: 7ced0dfc-fff1-4f9c-a5b4-e6fcd672bf9a
IP: 93.165.xxx.xxx
2026-08-25 08:41:29 UTC

Mit ID

John Richardt Søbjærg
inforevision statsautoriseret revisionsaktieselskab CVR: 19263096
Statsautoriseret revisor
På vegne af: inforevision a/s
Serienummer: 70a986b1-9464-4830-8fb8-b43b6517911a
IP: 93.165.xxx.xxx
2026-08-25 08:55:35 UTC

Mit ID