INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD FROM 16 MAY 2024 TO 15 MAY 2025 ON THE DESCRIPTION OF COMPAYAS SMS-SYSTEMS (CPSMS.DK, PROSMS.SE/SMS.DK OG SMS1919.DK) AND THE ASSOCIATED TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES AND OTHER CONTROLS, THEIR DESIGN AND OPERATIONAL EFFECTIVENESS RELATING TO THE PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE GENERAL DATA PROTECTION REGULATION AND THE DANISH DATA PROTECTION ACT

compaya© MOBILE SOLUTIONS

This English document is an unofficial translation of the original Danish assurance report, and in case of any discrepancy between the original Danish assurance report and the English translation, the Danish text shall prevail.

BDO

CONTENT

1. INDEPENDENT AUDITOR'S OPINION

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD FROM 16 MAY 2024 TO 15 MAY 2025 ON THE DESCRIPTION OF COMPAYAS SMS-SYSTEMS (CPSMS.DK, PROSMS.SE/SMS.DK OG SMS1919.DK) AND THE ASSOCIATED TECHNICAL AND ORGANISATIONAL SECURITY MEASURES AND OTHER CONTROLS, THEIR DESIGN AND OPERATIONAL EFFECTIVENESS RELATING TO THE PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE GENERAL DATA PROTECTION REGULATION AND THE DATA PROTECTION ACT

To: The management of Compaya A/S
Compaya A/S' Customers (data controllers)

Scope

We have been tasked with providing a declaration of the description prepared by Compaya A/S (the data processor) for the entire period from 16 May 2024 to 15 May 2025 in section 3 of Compaya's SMS-systems and the associated technical and organizational security measures and other controls, aimed at the processing and protection of personal data in accordance with the Regulation of the European Parliament and of the Council on the protection of natural persons in connection with the processing of personal data and on the free movement of such data (the General Data Protection Regulation) and the Act on Supplementary Provisions to the General Data Protection Regulation (the Data Protection Act), and on the design and operational effectiveness of the technical and organizational security measures and other controls linked to the control objectives stated in the description.

Responsibilities of the Data Processor

The data processor is responsible for preparing the statement in section 2 and the accompanying description, including the completeness, accuracy, and manner in which the statement and description are presented. The data processor is also responsible for providing the services covered by the description; stating the control objectives; and designing and implementing controls to achieve the stated control objectives.

Auditor independence and quality management

We have complied with the requirements of independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Guidelines for Auditors' Ethical Conduct (IESBA Code), which is based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct, as well as ethical requirements applicable in Denmark.

BDO Statsautoriseret revisionsaktieselskab applies the International Standard on Quality Management 1, ISQM 1, which requires us to design, implement and operate a quality management system, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable laws and other regulations.

Auditor's Responsibilities

Our responsibility is to express an opinion on the data processor'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 have performed our work in accordance with ISAE 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether the description is fairly presented, in all material respects, and whether the controls are suitably designed and operating effectively.

An assurance engagement to provide a statement on the description, design, and operational effectiveness of controls at a data processor involves performing procedures to obtain evidence about the information in the data processor's description and about the design and operational effectiveness of the controls. The selected

procedures depend on the data processor's auditor's judgment, including the assessment of the risks that the description is not fairly presented and that the controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls, that we consider necessary to provide a high level of assurance that the control objectives stated in the description were achieved. A report assignment of this type also includes evaluating the overall presentation of the description, the suitability of the control objectives stated therein and the suitability of the criteria specified and described by the data processor in section 2.

It is our opinion that the evidence obtained is sufficient and appropriate to provide a basis for our conclusion.

Limitations of controls at a data processor

The data processor's description is prepared to meet the common needs of a broad range of data controllers and therefore may not include all the aspects of the use of Compaya's SMS-systems that each individual data controller may consider important based on their specific circumstances. Furthermore, due to their nature, controls at a data processor may not prevent or detect all breaches of personal data security. Additionally, any projection of the assessment of the operational effectiveness of controls to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Conclusion

Our conclusion is based on the matters outlined in this report. The criteria we used in forming our conclusion are the criteria described in the data processor's statement in section 2. It is our opinion that:

a. that the description of Compaya's SMS-systems and the associated technical and organizational security measures and other controls aimed at the processing and protection of personal data in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act, as they were designed and implemented throughout the period 16 May 2024 to 15 May 2025, is fairly presented in all material respects, and

b. that the technical and organizational security measures and other controls related to the control objectives stated in the description were suitably designed throughout the period 16 May 2024 to 15 May 2025, and

c. the tested technical and organizational security measures and other controls, which were necessary to provide a high level of assurance that the control objectives in the description were achieved in all material respects, operated effectively throughout the period 16 May 2024 to 15 May 2025.

Description of tests of controls

The specific controls tested and the results of these tests are set out in section 4.

Intended users and purposes

This report is intended only for data controllers who have used the data processor's Compaya's SMS-systems and who have sufficient understanding to consider it along with other information, including the technical and organizational security measures and other controls that the data controllers themselves have implemented, when assessing whether the requirements of GDPR and the Danish Data Protection Act have been met.

Copenhagen, 03. July 2025

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

Mikkel Jon Larssen
Partner, Head of Risk Assurance, CISA, CRISC

2. COMPAYA A/S' STATEMENT

Compaya A/S processes personal data in connection with Compaya's SMS-systems for our customers who are data controllers in accordance with the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation) and the Act on Supplementary Provisions to the General Data Protection Regulation (the Danish Data Protection Act).

The accompanying description is prepared for use of data controllers who have used Compaya's SMS-systems and who have sufficient understanding to consider the description along with other information, including the technical and organizational security measures and other controls that the data controllers themselves have implemented, when assessing whether the requirements of GDPR and the Danish Data Protection Act have been complied with.

Compaya A/S uses sub-processors. The relevant control objectives and associated technical and organizational security measures and other controls of this sub-processor(s) are not included in the accompanying description.

Compaya A/S confirms that the accompanying description in section 3 provides a fair description of Compaya's SMS-systems and the associated technical and organizational security measures and other controls throughout the period 16 May 2024 to 15 May 2025. The criteria used to give this opinion were that the accompanying description:

1. Describe SMS-systems and how the associated technical and organizational security measures and other controls were designed and implemented, including an account of:
    - The types of services provided, including the type of personal data processed.
    - The processes in both IT systems and business procedures used to process personal data and, if necessary, to correct and delete personal data as well as to restrict the processing of personal data.
    - The processes used to ensure that the data processing carried out is in accordance with a contract, instruction or agreement with the data controller.
    - The processes that ensure that the persons authorised to process personal data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality.
    - The processes that, upon termination of data processing, that all personal data is deleted or returned to the data controller at the data controller's choice, unless the law or regulation requires the retention of the personal data. The processes, that in the event of a personal data breach, support the data controller in notifying the supervisory authority and informing the data subjects.
    - The processes that ensure appropriate technical and organizational security measures for the processing of personal data, considering the risks posed by processing, particularly accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
    - The controls, which we have assumed, with reference to the delimitation of SMS systems, would be designed and implemented by the data controllers, and which, if necessary to achieve the control objectives, are identified in the description.
    - The other aspects of the control environment, risk assessment process information systems and communication, control activities, and monitoring controls that have been relevant to the processing of personal data.

2. Does not leave out or misrepresent information relevant to the scope of Compaya's SMS-systems and the associated technical and organizational security measures and other controls, considering that this description prepared to meet the common needs of a broad range of data controllers and therefore cannot include every aspect of Compaya's SMS-systems that each individual data controller may consider important according to their particular circumstances.

Compaya A/S confirms that the technical and organizational security measures and other controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period 16 May 2024 to 15 May 2025. The criteria used to provide this statement were that:

1. The risks that threatened the achievement of the control objectives stated in the description were identified.

2. The identified controls, if performed as described, would provide a high level of assurance that the relevant risks would not prevent the achievement of the stated control objectives.

3. The controls were consistently applied as designed, including that manual controls were performed by persons with appropriate competence and authority, throughout the period 16 May 2024 to 15 May 2025.

Compaya A/S confirms that appropriate technical and organizational security measures and other controls have been implemented and maintained to meet agreements with the data Controllers, good data processing practices and relevant requirements for Data Processors in accordance with the GDPR and the Danish Data Protection Act.

Copenhagen, 03. July 2025

Compaya A/S

Martin Saldern Schrøder
Director/Partner

3. COMPAYA A/S' DESCRIPTION OF COMPAYA'S 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, and similar entities. Compaya is based in Copenhagen.

Compaya's approximately nine employees specialize in sales and marketing, system development, server operations, support, and information security. The organization is structured into a sales department and a development department.

The head of Information Security is responsible for managing Compaya's data protection relating to the processing activities carried out on behalf of its customers. This includes the conclusion of data processing agreements, responding to inquiries from data controllers, notifying data controllers of personal data breaches, and ensuring compliance with internal policies and procedures, among other duties.

SMS-systems and processing of personal data

Compaya provides its SMS systems as Software-as-a-Service (SaaS) solutions. To use the SMS systems, customers must accept the terms of service available on the respective websites of the systems. In some cases, customers request a specific master agreement, which is then prepared upon request. Through both the websites and the SMS systems, customers are encouraged to enter into a data processing agreement. This agreement is either generated electronically or, if needed, Compaya's standard data processing agreement is customized to the individual customer.

The SMS systems are developed at the company's office in Copenhagen but are operated from external hosting centers, which therefore function 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 about the data controller. This includes company name, address, name, email address, phone number, CVR number, and, where applicable, EAN number, as well as logs of activity related to the use of the SMS systems. This constitutes regular (non-sensitive) personal data.

Within the SMS systems, the data controller's users input personal data about recipients of SMS messages. This specifically includes mobile phone numbers and, in some cases, names. Additionally, data controllers may enter personal data directly into the body of the SMS message.

As a general rule, Compaya performs data processing in the form of storage and transmission of the SMS messages entered into the SMS systems by the data controllers. A log of the sent SMS messages is retained, and Compaya employees have access to the information contained in these messages via the user roles configured as system permissions. This access is used in connection with troubleshooting and support provided to the data controllers.

Management of personal data security

Compaya has established requirements for the development, implementation, maintenance, and continual improvement of a personal data security management system. This system is designed to ensure compliance with agreements made with data controllers, adherence to good data processing practices, and fulfillment of relevant obligations for data processors under the General Data Protection Regulation (GDPR) and the Danish Data Protection Act.

The technical and organizational security measures, and other controls implemented to protect personal data, are based on risk assessments and are designed to ensure confidentiality, integrity, and availability. These

measures also support compliance with applicable data protection legislation. Wherever 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 key areas, for which control objectives and control activities have been defined:

ARTICLE	AREA
Article 28, (1)	The data processor's guarantees
Article 28, (3)	Data processing agreement
Article 28, (3), (a and h), and (10) Artikel 29 Article 32, (4)	Instruction 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 controllers
Article 30, (2), (3) and (4)	Record of processing activities
Article 33, (2)	Notification of personal data breaches

Risk assessment

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

A continuous assessment is conducted to determine the appropriate level of security. This assessment considers risks related to accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of or access to personal data that is transmitted, stored, or otherwise processed.

As a basis for updating the technical and organizational security measures and other controls, a risk assessment is performed annually. The risk assessment evaluates the likelihood and consequences of events that may threaten personal data security and thereby the rights and freedoms of natural persons, including accidental, intentional, and unintentional incidents. The assessment considers the current technical level and implementation costs. As part of the risk assessment, a Data Protection Impact Assessment (DPIA) has been conducted for the SMS systems. Furthermore, Compaya has utilized the Risknon model from Risikoanalyser.dk for its risk analysis.

Technical and organizational security measures and other controls

The technical and organizational security measures and other controls apply 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 matrix are an integrated part of the subsequent description.

The data processor's guarantees

Compaya has implemented policies and procedures that ensure it can provide sufficient guarantees to implement appropriate technical and organizational security measures in a manner that complies with the requirements of the General Data Protection Regulation (GDPR) and ensures the protection of data subjects' rights.

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

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

Data processing agreements

Compaya has established a procedure for entering into data processing agreements that specify 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 about the use of sub-processors. The data processing agreements are signed by both parties and stored electronically.

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

As a data processor, Compaya immediately notifies the data controller if, in Compaya's opinion, any instruction conflicts with the GDPR, other EU data protection provisions, or the national laws of the Member States.

Sub-processors

The data processor has the general approval of the data controller to engage with sub-processors. However, the data processor must obtain approval from the data controller for any planned changes concerning the addition or replacement of sub-processors, thereby allowing the data controller the opportunity to object to such changes.

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

Each year, typically in March, the sub-processor must provide a statement for the preceding year from an approved auditing organization regarding the sub-processor's implementation of its own policies and the adequacy thereof.

Confidentiality and statutory duty of confidentiality

As a data processor, Compaya ensures that only individuals who are currently authorized have access to the personal data processed on behalf of the data controller. Access rights are immediately revoked upon expiration or withdrawal of the authorization.

Authorization is granted solely to individuals for whom access to personal data is necessary in order to fulfil the data processor's obligations towards the data controller.

Compaya further ensures that all authorised individuals have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality.

Upon request from the data controller, Compaya is able to demonstrate that the relevant personnel are subject to the aforementioned duty of confidentiality.

Technical and organizational security measures

Risk assessment
Compaya has implemented technical and organizational security measures based on an assessment of the risks related to confidentiality, integrity, and availability of personal data. A reference is made to a separate section detailing this assessment.

Contingency planning
Compaya has established contingency plans to ensure the timely restoration of availability and access to personal data in the event of physical or technical incidents. A crisis response framework has been implemented and is activated in such cases. A crisis management team has been appointed, and formal procedures have been established for initiating the crisis response.

Compaya has developed detailed contingency and recovery plans for systems and data. These plans are made available via Dropbox. The plans are regularly tested and updated in connection with changes to systems and related infrastructure.

Storage of personal data
Compaya has implemented procedures to ensure that the storage of personal data is carried out solely in accordance with Compaya's data protection policy. Access to personal data is granted based on a work-related need and in accordance with the principle of need-to-know.

Physical access control
Compaya has implemented procedures to ensure that premises are protected against unauthorized physical access. Compaya does not operate secured facilities such as server rooms and therefore does not utilize access control systems such as key cards. Customers, suppliers, and other visitors are accompanied at all times. Outside of normal working hours, entry to the premises requires a code for the alarm system.

Compaya utilizes hosting providers for all server infrastructure. Compaya does not have physical access to the facilities of these hosting providers. Access to such facilities is restricted to authorized personnel employed by the respective hosting providers.

Logical access control
Compaya has implemented controls to ensure that access to systems and data is protected against unauthorized access to personal data. Each user is assigned a unique user ID and password, and access to resources and systems is granted based on this identification. All access rights are allocated according to a work-related need-to-know principle.

At least once annually, an evaluation is conducted to assess whether users continue to require access based on their job responsibilities, including a review of the relevance and accuracy of assigned user rights. Procedures and controls support the processes for user creation, modification, deactivation, and access rights management, including periodic reviews.

Requirements regarding password length and complexity, as well as account lockout following unsuccessful login attempts, are defined in accordance with best practices for secure logical access control. Technical measures have been implemented to enforce these requirements.

Remote workstations and remote access to systems
Compaya has implemented procedures to ensure that access from workstations located outside of Compaya's premises, as well as remote access to servers and data, is conducted via secure VPN connections. Furthermore, Compaya has implemented procedures to ensure that external communication channels are protected through encryption.

Network security
Compaya has implemented procedures to ensure the secure use and operation of its networks. The production network is hosted by team.blue Denmark A/S (Zitcom/Curanet/Wannafind) and Rackhosting ApS and is segregated from Compaya's office network. Access between these networks is restricted to the extent possible and is managed in accordance with the procedures described above. At Compaya's premises on Palægade, only equipment related to the office network is present, which is segmented into VLANs.

The office network at Compaya's Palægade 4 location is protected by a firewall integrated into the router, which is configured to block all inbound traffic and allow all outbound traffic. All desktop and laptop computers are additionally protected by a software firewall provided through Bitdefender Endpoint Security.

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

Antivirus software and system patches
Compaya has implemented procedures to ensure that all devices with access to networks and applications are protected against viruses and malware. Antivirus software and other protective systems are continuously updated and adjusted in accordance with the prevailing threat landscape.

Compaya has also implemented procedures to ensure that system software is regularly updated in accordance with vendor specifications and recommendations. The patch management procedures cover operating systems, critical services, and relevant software installed on servers and workstations.

Data backup and recovery
Compaya has implemented procedures to ensure that systems and data are backed up to mitigate the risk of data loss or loss of availability in the event of a system failure. Backup copies are stored at an alternative location. Restore tests of the backup are performed on an ongoing basis, and at a minimum, once per year.

Logging of personal data
Compaya has implemented procedures to ensure that logging is configured in accordance with legal requirements and business needs, based on a risk assessment of systems and the prevailing threat landscape. The scope and quality of log data are sufficient to identify and demonstrate any misuse of systems or data. Log data is continuously reviewed for relevance and indications of abnormal behaviour. All log data is securely protected.

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

Disposal of IT equipment
Storage media designated for destruction may be handed over to the IT Security Officer or the Head of IT Development, who is responsible for ensuring the effective and permanent destruction of the media or the data contained therein.

Data protection by design and by default

Compaya has implemented policies and procedures for the development and maintenance of its SMS systems to ensure a controlled change management process. A formal Change Management procedure is used to govern all development and change tasks, each of which follows a standardized process.

Development, testing, and production environments are separated, and all development and change tasks undergo a structured testing phase. Procedures for version control, logging, and backup have been established to enable the reinstallation of previous versions when necessary.

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 such data ceases upon termination of the contract with the data controller.

Assistance to the data controllers

Compaya has implemented policies and procedures to ensure that it can assist the data controller in fulfilling its obligation to respond to data subjects' requests to exercise their rights.

Compaya has also implemented policies and procedures to ensure that it can assist the data controller in complying with its obligations under Article 32 on the security of processing, Article 33 on notification of personal data breaches, and Articles 34 to 36 concerning data protection impact assessments.

Furthermore, Compaya has implemented policies and procedures to ensure that it can make all information necessary to demonstrate compliance with the requirements applicable to data processors available to the data controller. Compaya also enables and contributes to audits, including inspections, conducted by the data controller or by another auditor authorized by the data controller.

Record 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. This record is updated regularly and reviewed as part of the annual review of policies, procedures, and related documentation. 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 documented with detailed information about the incident, and that the data controller is notified without undue delay after Compaya becomes aware of the breach.

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 informed.

Complementary controls implemented by the data controller

As part of the delivery of services, certain controls are assumed to be implemented by the data controller, which are essential for achieving the control objectives described in this document.

The data controller is, among other things, responsible for:

- Ensuring that the instructions set out in the data processing agreement are lawful under the applicable data protection legislation at all times.
- Ensuring that the instructions in the data processing agreement are appropriate in relation to the core service.
- Ensuring that the administrators' use of the SMS systems and the processing of personal data within the systems are carried out in compliance with data protection legislation.
- Ensuring that any specific requirements for security measures on the part of the data controller are described in the data processing agreement.
- Ensuring that the data controller's users in the SMS systems are kept up to date.

4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND TEST RESULTS

Purpose and scope

BDO has carried out its work in accordance with ISAE 3000 on assurance engagements other than auditing or reviewing historical financial information.

BDO has carried out actions to obtain evidence of the information in Compaya A/S' description of Compaya's SMS-systems as well as of the design of the associated technical and organisational security measures and other controls. The chosen actions depend on BDO's assessment, including the assessment of the risks that the description is not fair and that the controls are not appropriately designed.

BDO's testing of the design of technical and organisational security measures and other controls as well as their implementation has included the control objectives and associated control activities selected by Compaya A/S and which appear in the subsequent control chart.

In the control form, BDO has described the tests carried out that were deemed necessary in order to obtain a high degree of assurance that the stated control objectives were achieved and that the associated controls were appropriately designed in the period 16 May 2024 to 15 May 2025.

Performed test actions

Testing of the design of technical and organisational security measures and other controls as well as their implementation has been carried out by inquiry, inspection and observation.

Type	Description
Query	Inquiries with appropriate personnel have been carried out for all essential control activities. The queries were carried out in order to, among other things, obtain knowledge and further information on policies and procedures in place, including how the control activities are carried out, as well as to confirm evidence of policies, procedures and controls.
Inspection	Documents and reports indicating the performance of the controls are reviewed for the purpose of assessing the design and monitoring of the specific controls, including whether the controls are designed to be effective if implemented, and whether the controls are adequately monitored and controlled at appropriate intervals. Tests of essential system setups of technical platforms, databases and network equipment have been carried out to ensure that controls have been implemented, including, for example, assessment of logging, backups, patch management, authorizations and access controls, data transmission and inspection of equipment and locations.
Observation	The use and existence of specific controls have been observed, including tests to ensure that the controls are implemented.

For the services provided by Rackhosting ApS within hosting, we have received an ISAE 3000 report for the period 1. May 2023 to 30. April 2024 for the sub-processor's technical and organisational security measures and other controls and an ISAE 3402 report for the general it-controls for the period 1. May 2023 to 30. April 2024.

For the services provided by Team.blue Denmark A/S (Zitcom/Curanet/Wannafind) within hosting, we have received an ISAE 3402 report for the sub-processor's technical and organisational security measures and other controls.
For the services provided by Curanet A/S within hosting, we have received an ISAE 3402 report for the sub-processor's technical and organisational security measures and other controls.

The relevant control objectives and associated controls of this sub-processors are not included in Compaya A/S' description of Compaya's SMS-systems and the associated technical and organisational security

measures and other controls. Thus, we have only inspected the documentation received and tested the controls at Compaya A/S that ensure the performance of a proper supervision of the sub-processor's compliance with the data processing agreement entered into between the sub-processor and the data processor and compliance with the General Data Protection Regulation and the Data Protection Act.

Test result

The results of the tests carried out on technical and organisational security measures and other controls indicate whether the described tests have given rise to the detection of deviations.

A deviation exists when:

- Technical or organisational security measures or other controls have yet to be designed and implemented in order to meet a control objective.
- Technical or organisational security measures or other controls linked to a control objective are not appropriately designed, implemented or effective.

Article 28, stk. 1: Guarantees of the processor		
Control objectives ▶ *Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control activity	**Tests conducted by BDO**	**Test result**
Information security policies and information security policy review The data processor's management has approved a written information security policy, The IT security policy is based on the risk assessment carried out. An assessment is made on an ongoing basis – and at least once a year – of whether the IT security policy needs to be updated.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that there is an information security policy that the management has reviewed and approved. We have inspected that procedures have been updated and approved during the declaration period.	No exceptions noted.
Information security policies in accordance with data processing agreements The management of the data processor has ensured that the information security policy is not in conflict with the concluded data processing agreements.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected documentation for the management's assessment that the information security policy generally meets the requirements for security measures and processing security in entered into data processing agreements. We have randomly inspected that the requirements in the data processing agreements entered into are not in conflict with the information security policy.	No exceptions noted..
Recruitment of employees – Screening A review of the data processor's employees is carried out in connection with employment. The verification shall include, where appropriate: • References from previous employments • CV • Diplomas	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that there are formalised procedures in place to ensure verification of the data processor's employees in connection with employment.	We have established that a formalised procedure for candidate screening is in place. However, as there have been no new hires during the reporting period, we have not been able to test the implementation and effectiveness of the control. No exceptions noted..

Article 28, stk. 1: Guarantees of the processor		
Control objectives ▶ *Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control activity	**Tests conducted by BDO**	**Test result**
Termination of employees - withdrawal of access rights and assets Upon resignation, a process has been implemented by the data processor to ensure that the user's rights become inactive or cease, including that assets are confiscated.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected procedures that ensure that the rights of resigned employees are inactivated or terminated upon resignation, and that assets such as access cards, PCs, mobile phones, etc. are confiscated.	We have established that a formalised procedure for employee termination is in place. However, as there have been no terminations during the reporting period, we have not been able to test the implementation and effectiveness of the control. No exceptions noted..
Resignation of employees - information about confidentiality and professional secrecy Upon resignation, the employee is informed that the signed confidentiality agreement is still in force and that the employee is subject to a general duty of confidentiality in relation to the processing of personal data that the data processor performs for the data controllers.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that the data processor has designed a formalized procedure ensuring employees are subjects to confidentiality upon resignation.	We have established that a formalised procedure regarding confidentiality after termination is in place. However, as there have been no terminations during the reporting period, we have not been able to test the implementation and effectiveness of the control. No exceptions noted.
Awareness, education and training regarding information security Ongoing awareness training is carried out of the data processor's employees in relation to IT security in general and processing security in relation to personal data.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that the data processor offers awareness training to employees covering general IT security and processing security in relation to personal data. We have inspected documentation that all employees who either have access to or process personal data have completed the offered awareness training.	No exceptions noted.

Article 28, stk. 3, article 29, article 30 stk. 2, 3 and 4 and article 32 stk. 4: Data processing agreement and processing of personal data on behalf of the data controller's instructions		
Control objectives ▶ *Procedures and controls are complied with to ensure that instructions regarding the processing of personal data are complied with in accordance with the incoming data processing agreement.*		
Control activity	**Tests conducted by BDO**	**Test result**
Procedure for processing personal data There are written procedures that stipulate that personal data processing may only be carried out when there is an instruction. An ongoing assessment is conducted – at least once a year – to determine whether the procedures need to be updated.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that there is a formalized procedure in place to ensure that the processing of personal data only takes place in accordance with instructions. We have inspected that the procedure includes a requirement for a minimum annual assessment of the need for updating, including changes in the data controller's instructions or changes in data processing. We have inspected that in the reporting period the procedure is updated and management approved.	No exceptions noted.
Compliance with instructions for processing personal data The data processor only performs the processing of personal data that is stated in the instructions from the data controller.	We have conducted inquiries with appropriate personnel at the data processor. We have randomly inspected data processing agreements entered into with data controllers and observed that the agreements contain instructions from data controllers. We have inspected the data processor's record of processing activities and by random inspection inspected that the processing is carried out in accordance with instructions from the data controller in the reporting period.	No exceptions noted.
Notification of the data controller in the event of an illegal instruction he data processor immediately notifies the data controller if an instruction, in the data processor's opinion, is in conflict with the GDPR or other EU or member state national data protection regulations.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected the data processor's template for entering into data processing agreements with the data controller and randomly concluded data processing agreements with a data controller and observed that the data processor is obliged to notify the	We have found that there have been no cases where instructions have been assessed as contrary to legislation. We have therefore not been able to test the control for implementation and efficiency. No exceptions noted..

Article 28, stk. 3, article 29, article 30 stk. 2, 3 and 4 and article 32 stk. 4: Data processing agreement and processing of personal data on behalf of the data controller's instructions		
Control objectives ▶ *Procedures and controls are complied with to ensure that instructions regarding the processing of personal data are complied with in accordance with the incoming data processing agreement.*		
Control activity	**Tests conducted by BDO**	**Test result**
	Upon inquiry, we have been informed that there have been no cases during the declaration period where instructions have been assessed as contrary to legislation.	

Article 28, stk. 3, litra c: Storage of personal data		
Control objectives ▶ *Procedures and controls are complied with to ensure that the data processor only stores personal data in accordance with the agreement with the data controller.*		
Control activity	**Tests conducted by BDO**	**Test result**
Storage of information is in accordance with the data controller's requirements There are written procedures that include requirements for the storage of personal data solely in accordance with the agreement with the data controller. Ongoing assessments are conducted – at least once a year – to determine whether the procedures need to be updated.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that there are formalised procedures for only storing and processing personal data in accordance with the data processing agreements. We have inspected the storage of personal data by random samples and ensured that personal data is only stored for the period agreed with the data controller. We have inspected that the procedures have been updated and approved during the reporting period.	No exceptions noted.
Location of processing and storage of information The data processor's data processing, including storage, may only take place at locations, countries, or territories approved by the data controller.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that the data processor has a comprehensive and updated overview of processing activities with an indication of locations, countries or areas of land for the processing and storage of personal data. We have randomly inspected data processing from the data processor's overview of processing activities to ensure that there is documentation that the data processing, including storage of personal data, is only carried out at the locations stated in the data processing agreement – or has otherwise been approved by the data controller.	No exceptions noted.

Article 28. stk. 2 and 4: Sub-processors

Control objectives

- *Procedures and controls are complied with to ensure that only approved sub-processors are used, and that the data processor ensures satisfactory processing security when following up on their technical and organisational measures to protect the rights of the data subjects and the processing of personal data.*

Control activity	Tests conducted by BDO	Test result
Sub-data processing agreement and instructions There are written procedures that contain requirements for the data processor when using sub-processors, including requirements for sub-data processing agreements and instructions. Ongoing assessments are conducted – at least once a year – to determine whether the procedures need to be updated.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that there are formalised procedures for the use of sub-processors, including requirements for sub-data processing agreements and instructions. We have inspected that the procedures have been updated and approved during the declaration period.	No exceptions noted.
Approval of sub-processors The Data Processor only uses sub-processors for the processing of personal data that has been specifically or generally approved by the Data Controller.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that the data processor has a comprehensive and updated overview of the sub-processors used. We have randomly inspected sub-processors from the data processor's overview of sub-processors to ensure that there is documentation that the sub-processors' data processing is stated in the data processing agreements entered into with the data controller.	No exceptions noted.
Changes in approved sub-processors In the event of changes in the use of generally approved sub-processors, the data controller is notified in a timely manner to allow for objections and/or the withdrawal of personal data from the data processor. In the event of changes in the use of specifically approved sub-processors, this is approved by the data controller.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that there are formalised procedures for notifying the data controller of changes in the use of sub-processors. Upon inquiry, we have been informed that there have been no changes to sub-processors during the declaration period.	We have found that there have been no changes to sub-processors. We have therefore not been able to test the control for implementation and efficiency. No exceptions noted..

Article 28. stk. 2 and 4: Sub-processors

Control objectives

- *Procedures and controls are complied with to ensure that only approved sub-processors are used, and that the data processor ensures satisfactory processing security when following up on their technical and organisational measures to protect the rights of the data subjects and the processing of personal data.*

Control activity	Tests conducted by BDO	Test result
The subprocessor's obligations The Data Processor has imposed on the sub-processor the same data protection obligations as those provided for in the Data Processing Agreement or similar with the Data Controller.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that data processing agreements have been entered into with the sub-processors used, We have randomly inspected sub-data processing agreements to ensure that they contain the same requirements and obligations as are stated in the data processing agreements between the data controllers and the data processor.	No exceptions noted.
Overview of sub-processors The data processor has a list of approved sub-processors stating: • Name • CVR no. • Address • Description of the processing	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that the data processor has a comprehensive and updated overview of used and approved sub-processors. We have inspected that the overview contains at least the required information about the individual sub-processors.	No exceptions noted.
Supervision of sub-processors On the basis of an updated risk assessment of the individual sub-processor and the activity carried out by the sub-processor, the data processor conducts an ongoing follow-up of this at meetings, inspections, review of the audit statement or similar. The data controller is informed of the follow-up that has been carried out at the sub-processor.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected documentation that a risk assessment has been made of the individual sub-processor and the current processing activity of the sub-processor. We have inspected that the data processor has carried out supervision, including obtaining and reviewing the sub-data processor's auditor's statements, certifications and the like. We have inspected that the data processor's supervision of sub-processors has not given rise to any further action.	No exceptions noted.

Article 28. stk. 2 and 4: Sub-processors		
Control objectives ▶ *Procedures and controls are complied with to ensure that only approved sub-processors are used, and that the data processor ensures satisfactory processing security when following up on their technical and organisational measures to protect the rights of the data subjects and the processing of personal data.*		
Control activity	**Tests conducted by BDO**	**Test result**
	We have inspected documentation that the data processor has informed the data controller of the follow-up carried out by the sub-data processor.	

Article 28, stk. 3, litra b: Confidentiality and statutory professional secrecy		
Control objectives ▶ *Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to ensure relevant processing security.*		
Control activity	**Tests conducted by BDO**	**Test result**
Recruitment of employees - Non-disclosure agreement with employees and introduction to information security Upon employment, employees sign a confidentiality agreement. Furthermore, the employee is introduced to information security policy and procedures regarding data processing as well as other relevant information in connection with the employee's processing of personal data.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that the data processor has a process for confidentiality and non-disclosure agreements.	We have established that a formalised procedure regarding confidentiality agreements upon new hires is in place. However, as there have been no new hires during the reporting period, we have not been able to test the implementation and effectiveness of the control. No exceptions noted.

Article 28, stk. 3, litra c: Technical and organisational security measures		
Control objectives ▶ *Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activity	**Tests conducted by BDO**	**Test result**
Agreed security measures There are written procedures that require that agreed safeguards are put in place for the processing of personal data in accordance with the agreement with the data controller. An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that formalised procedures are in place to ensure that the agreed security measures are put in place. We have inspected that procedures have been updated and approved during the declaration period.	No exceptions noted.
Risk assessment The data processor has conducted a risk assessment and, on the basis of this, implemented the technical measures that are deemed relevant to achieve appropriate security, including the establishment of the security measures agreed with the data controller.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that the data processor has carried out a risk assessment based on potential risks to the accessibility, confidentiality and integrity of the data subject in relation to the rights of the data subject. We have inspected that the risk assessment carried out has been updated and approved. We have randomly inspected that the data processor has implemented technical measures based on the risk assessment, including measures agreed with the data controller.	No exceptions noted.
Antivirus Antivirus is installed for the workstations and systems used for the processing of personal data, which is continuously updated.	We have conducted inquiries with appropriate personnel at the data processor. We have randomly inspected that for PCs used for the processing of personal data, antivirus has been installed that has been updated.	No exceptions noted.

Article 28, stk. 3, litra c: Technical and organisational security measures		
Control objectives ▶ *Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activity	**Tests conducted by BDO**	**Test result**
Conditional access - access to personal data Access to personal data is isolated to users with a work-related need for it.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that formalised procedures are in place to restrict users' access to personal information. We have inspected that the agreed technical measures support the maintenance of the restriction on users' work-related access to personal data.	No exceptions noted.
Monitoring of systems and environments For the systems and databases used for the processing of personal data, system monitoring with alarms has been established. The monitoring includes: • RAM and storage usage • MySQL connections • Up time (Pingdom)	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that systems and databases used for the processing of personal data have established system monitoring with alarms.	No exceptions noted.
Encryption for the transmission of personal data Effective encryption is used when transmitting confidential and sensitive personal data via the internet and by e-mail.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected the use of encryption for transmissions of sensitive and confidential personal data via the internet or by e-mail.	No exceptions noted.
Logging Logging has been established in systems, databases and networks for the following conditions: • Activities performed by users • Activities of System Administrators and Others with Special Rights • Security incidents include:	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that logging of user activities in systems, databases and networks used for the processing and transmission of personal data is configured and enabled.	No exceptions noted.

Article 28, stk. 3, litra c: Technical and organisational security measures		
Control objectives ▶ *Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activity	**Tests conducted by BDO**	**Test result**
o Failed log-in attempts to systems	We have inspected that logs have the expected content in relation to setup. We have inspected that logs with system administrators and others with special rights activities have the expected content in relation to setup.	
Vulnerability scans and penetration tests The established technical measures are continuously tested by vulnerability scans and penetration tests.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that formalised procedures are in place for ongoing testing of technical measures, including the conduct of vulnerability scans and penetration tests. We have inspected by random checks that there is documentation of ongoing tests of the established technical measures. We have inspected that any deviations and weaknesses in the technical measures have been dealt with or accepted in a timely manner and satisfactorily.	No exceptions noted.
System Software Maintenance Changes to systems, workstations, databases, and networks follow established procedures that ensure maintenance with relevant updates and patches, including security patches.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected by extraction that databases and networks are updated with relevant updates and security patches. We have randomly inspected that workstations are updated with the latest system update.	No exceptions noted.
Conditional Access - procedure and periodic review There is a formalised procedure for granting and terminating user access to personal data. Users' access is regularly reviewed, including that rights can still be justified by a work-related need.	We have conducted inquiries with appropriate personnel at the data processor.	We have established that a formalised procedure for access assignment and discontinuing is in place. However, as there have been no new hires or terminations during the reporting period, we have not been able to test the implementation and effectiveness of the control.

Article 28, stk. 3, litra c: Technical and organisational security measures		
Control objectives ▶ *Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activity	**Tests conducted by BDO**	**Test result**
	We have inspected that formalised procedures are in place for granting and discontinuing users' access to systems and databases used for the processing of personal data. We have inspected the data processor's annual cycle / procedure for user management and observed that the data processor must regularly assess and approve assigned user access. We have inspected that the data processor has assessed and approved user access.	No exceptions noted.
Logical access control The data processor has established rules for password requirements that must be followed by everyone with access to personal data.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that users' access to carry out the processing of personal data is done through passwords that reflect the risk of the processing activity.	No exceptions noted.
Physical access control Physical access security has been established so that only authorised persons can gain physical access to premises and data centres in which personal data is stored and processed.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that formalised procedures are in place to ensure that only authorised persons can gain physical access to the data processor's premises. We have inspected documentation that only authorised persons have physical access to premises in which personal data is stored and processed. Upon inquiry, we have been informed that the data processor's personal data is stored with a hosting provider. We have inspected hosting provider's audit statement and observed that the statement is unqualified and that the statement does not contain matters regarding physical access security that have required further action from the data processor.	No exceptions noted.
Backup and restoration		No exceptions noted.

Article 28, stk. 3, litra c: Technical and organisational security measures		
Control objectives ▶ *Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant processing security.*		
Control activity	**Tests conducted by BDO**	**Test result**
The Data Processor has established a procedure for backup and re-establishment of data and systems that ensures that relevant systems and data are backed up and stored at another physical location, and that systems and data can be re-established.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that formalised procedures are in place to ensure backup and restoration of relevant data and systems, and that backups are stored in another physical location. We have inspected that backups of relevant systems and data are made in accordance with the procedure. We have inspected that backups have been restored during the declaration period.	
Remote workplaces and remote access to systems and data Remote access to the data processor's systems and data is via VPN connection.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected the data processor's network topology and observed that remote access to systems and data can only be achieved through VPN. We have inspected documentation that access to the VPN connection is done via two-factor authentication.	No exceptions noted.
Repair, service and destruction of IT equipment The Data Processor has established a procedure for repair, service and destruction of IT equipment that ensures secure handling of IT equipment containing personal data.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that the data processor has formalised procedures for repair, service and destruction of IT equipment. Upon inquiry, we have been informed that no IT equipment has been sent for repair, service or destruction.	We have established that the data processor has not sent IT equipment for repair, service or destruction. We have therefore not been able to test the control for implementation and efficiency. No exceptions noted.

Article 25: Data protection by design and default settings		
Control objectives ▶ *Procedures and controls are complied with to ensure information security and data protection are planned and implemented in the data processor's development and change process.*		
Control activity	**Tests conducted by BDO**	**Test result**
Change management and privacy-by-design The Data Processor has established a procedure for development and change tasks that ensures compliance with the privacy-by-design principles, and that all development and change tasks follow a formalized process that ensures testing and requirements for approval before implementation.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that the data processor has established a procedure for development and modification tasks that ensures compliance with the privacy-by-design principles, and that all development and modification tasks follow a formalized process that ensures testing and requirements for approval before implementation. We have randomly inspected for implemented changes that compliance with the privacy-by-design principles has been ensured in the change tasks. We have also inspected that the tasks have followed the formalised procedure, and that tests have been carried out and that the changes have been approved before implementation.	No exceptions noted.
Implementing change in the production environment The data processor has established a procedure for implementing changes in the production environment that ensures segregation of duties in the implementation process.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that there is a segregation of duties so that developers cannot implement changes directly in the production environment without a formal approval.	No exceptions noted.
Separation of the development, test, and production environment Development and testing are performed in development environments that are separate from production environments.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that development, testing and production environment are separate.	No exceptions noted.

Article 28, stk. 3, litra g: Deletion and return of personal data		
Control objectives ▶ *Procedures and controls are complied with to ensure that personal data can be deleted or returned if an agreement is entered into with the data controller.*		
Control activity	**Tests conducted by BDO**	**Test result**
Deletion of information in accordance with the data controller's requirements There are written procedures that require that personal data is stored and deleted in accordance with the agreement with the data controller. Ongoing assessments are conducted – at least once a year – to determine whether the procedures need to be updated.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that formalised procedures are in place for the storage and deletion of personal data in accordance with the agreement with the data controller. We have inspected that the procedures have been updated and approved during the declaration period.	No exceptions noted.
Requirements for the storage and deletion period of data are in accordance with the data controller's requirements The following specific requirements have been agreed for the data processor's storage periods and deletion routines.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that the available procedures for storing and deleting personal data contain specific requirements for the data processor's retention periods and deletion routines. We have inspected by random samples of data processing from the data processor's record of processing activities to ensure that there is documentation that personal data is stored in accordance with the agreed retention periods.	No exceptions noted.
Deletion and return upon termination of customer relationship Upon termination of processing of personal data by the Data Controller, data in accordance with the agreement with the Data Controller are: • Returned to the Data Controller, and/or • Deleted where it does not conflict with other legislation.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that formalised procedures are in place for the return and/or deletion of the data controller's data upon cessation of processing of personal data. Upon inquiry, we have been informed that it is individually agreed with the customer how the treatment is carried out.	We have established that there has been no termination of data processing agreements. We have therefore not been able to test the control for implementation and efficiency. No exceptions noted.

Article 28, stk. 3, litra g: Deletion and return of personal data		
Control objectives ▶ *Procedures and controls are complied with to ensure that personal data can be deleted or returned if an agreement is entered into with the data controller.*		
Control activity	**Tests conducted by BDO**	**Test result**
	Upon inquiry, we have been informed that there has been no termination of data processing agreements.	

Article 28, stk. 3, litra e, f and h: Assistance to the controller		
Control objectives ▶ *Procedures and controls are complied with to ensure that the data processor can assist the data controller with the disclosure, correction, deletion or restriction of information about the processing of personal data to the data subject.*		
Control activity	**Tests conducted by BDO**	**Test result**
Procedure for fulfilling the rights of data subjects There are written procedures that require the data processor to assist the data controller in relation to the rights of the data subjects. Ongoing assessments are conducted – at least once a year – to determine whether the procedures need to be updated.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that there are formalised procedures in place for the data processor's assistance of the data controller in relation to the rights of the data subjects. We have inspected that the procedures have been updated and approved.	No exceptions noted.
Technical measures for the fulfilment of data subjects' rights The data processor has established procedures which, to the extent agreed, enable timely assistance to the data controller in relation to the disclosure, correction, deletion or restriction of, and information about the processing of, personal data to the data subject.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that the available procedures for assistance to the data controller contain detailed procedures for: • Disclosure of information • Correction of information • Deletion of information • Restriction of processing of personal data • Information about the processing of personal data for the data subject. We have inspected evidence that the systems used support the implementation of the detailed procedures mentioned. Upon inquiry, we have been informed that no request for assistance has been made in relation to the rights of the data subjects in the reporting period.	We have established that there has been no request for assistance in relation to the rights of the data subjects. We have therefore not been able to test the control for implementation and efficiency. No exceptions noted.

Article 30(2), (3) and (4): List of categories of processing activities		
Control objectives ▶ *Procedures and controls are complied with to ensure that instructions regarding the processing of personal data are complied with in accordance with the incoming data processing agreement.*		
Control activity	**Tests conducted by BDO**	**Test result**
Record of processing activities The Data Processor has established a list of categories of processing activities as a Data Processor. The list must include: • the name and contact details of the data controller; • the categories of processing carried out on behalf of the controllers; • the name and contact details of each sub-processor; • indication of any transfer of personal data to a third country. The record shall be kept electronically and shall be made available to the supervisory authority upon request.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected the data processor's record of processing activities as a data processor and observed that it contains relevant information and that the record is stored electronically. We have inspected that the record has been updated and/or approved. Upon inquiry, we have been informed that the Danish Data Protection Agency has not requested disclosure of the list during the reporting period.	We have established that the Danish Data Protection Agency did not request disclosure of the list at the time of the declaration. We have therefore not been able to test the control for implementation and efficiency. No exceptions noted.

Article 33, stk. 2: Notification of personal data breaches		
Control objectives ▶ *Procedures and controls are complied with to ensure that any security breaches can be handled in accordance with the data processing agreement entered into.*		
Control activity	**Tests conducted by BDO**	**Test result**
Notification of personal data breaches There are written procedures that require the data processor to notify the data controllers in the event of a personal data breach. An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that there are formalized procedures that contain requirements for notifying the data controllers in the event of a personal data breach. We have inspected that the procedure has been updated and approved during the reporting period.	No exceptions noted.
Identification of personal data breaches The Data Processor has established the following controls for the identification of any personal data breaches: • Awareness among employees	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that the data processor provides awareness training to employees in relation to the identification of any personal data breaches.	No exceptions noted.
Timely notification of personal data breaches In the event of any personal data breaches, the Data Processor has notified the Data Controller without undue delay and no later than 24 hours after becoming aware that a personal data breach has occurred at the Data Processor or a sub-data processor.	We have conducted inquiries with appropriate personnel at the data processor. We have inspected that the data processor has an overview of security incidents with an indication of whether the individual incident has resulted in a breach of personal data security. We have observed that no incidents have been identified that have led to personal data breaches during the reporting period.	We have found that no incidents have been identified that have led to a breach of personal data security. We have therefore not been able to test the control for implementation and efficiency. No exceptions noted.
Assistance to data controllers in the event of a personal data breach The Data Processor has established procedures for assistance to the Data Controller in its notification to the Danish Data Protection Agency:	We have conducted inquiries with appropriate personnel at the data processor.	We have found that no incidents have been identified that have led to a breach of personal data security. We have therefore not been able to test the control for implementation and efficiency.

Article 33, stk. 2: Notification of personal data breaches		
Control objectives ▶ *Procedures and controls are complied with to ensure that any security breaches can be handled in accordance with the data processing agreement entered into.*		
Control activity	**Tests conducted by BDO**	**Test result**
• The nature of the personal data breach • Likely consequences of the personal data breach • Measures that have been taken or are proposed to be taken to deal with the personal data breach.	We have inspected that the procedures available for notifying data controllers in the event of a personal data breach contain detailed procedures for: • Description of the nature of the personal data breach • Description of the likely consequences of the personal data breach • Description of measures taken or proposed to be taken to deal with the personal data breach. We have inspected documentation that in the event of a personal data breach, measures have been taken to deal with the personal data breach. We have observed that no incidents have been identified that have led to personal data breaches during the reporting period.	No exceptions noted.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

VESTRE RINGGADE 28

8000 AARHUS C

www.bdo.dk

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/Partner
På vegne af: Compaya
Serienummer: e227fbdb-8ee7-42c5-94e0-69223948aaf3
IP: 2.66.xxx.xxx
2025-07-04 08:55:28 UTC

Mikkel Jon Larssen
BDO Holding VII, statsautoriseret revisionsaktieselskab CVR: 20222670
Partner, chef for Risk Assurance, CISA, CRISC
På vegne af: BDO
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 77.243.xxx.xxx
2025-07-04 08:56:46 UTC

Nicolai Tobias Visti Pedersen
BDO Holding VII, statsautoriseret revisionsaktieselskab CVR: 20222670
Statsautoriseret revisor
På vegne af: BDO
Serienummer: 375cad19-f0ea-4e39-8646-d3d882b8ce8e
IP: 37.96.xxx.xxx
2025-07-04 08:58:01 UTC

Penneo dokumentnøgle: 8JC2Z-T8AJZ-G0IVK-3FDKQ-QFCSI-YSGD6