



COMPAYA A/S

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT AT 15 MAY 2023 ON THE DESCRIPTION OF COMPAYAS SMS SYSTEMS (CPSMS.DK, PROSMS.SE/SMS.DK) AND RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH ACT ON SUPPLEMENTARY PROVISIONS

CONTENTS

1. INDEPENDENT AUDITOR'S REPORT	2
2. COMPAYA A/S' STATEMENT	4
3. COMPAYA A/S' DESCRIPTION OF THE SMS-SYSTEMS	6
CompAYA A/S	6
SMS Systems and processing of personal data.....	6
Management of the security of personal data	6
Risk Assessment	7
Technical and Organisational Security Measures and Other Controls.....	7
Complementary controls with the Controller	11
4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND THE RESULT OF TESTS	12
Article 28 (1): The Processor's guarantees	14
Article 28 (3): Data processor agreement	17
Article 28 (3) and (10), article 29 and article 32 (4): Instruction for processing of personal data	18
Article 28 (2) and (4): Subprocessors.....	19
Article 28 (3)(b): Confidentiality and professional secrecy	21
Article 28 (3)(c): Technical and organisational security measures.....	22
Article 25: Data protection by design and by default.....	29
Article 28 (3)(g) - Deletion of personal data	30
Article 28 (3)(e)(f)(h): Assistance to the Controller	31
Article 30 (2) (3) (4): Records of processing activities.....	34
Article 33 (2): Communication of personal data breach.....	35

1. INDEPENDENT AUDITOR'S REPORT

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT AT 15 MAY 2023 ON THE DESCRIPTION OF COMPAYAS SMS-SYSTEMS (CPSMS.DK, PROSMS.SE/SMS.DK) AND OF THE COMPANY AND RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH ACT ON SUPPLEMENTARY PROVISIONS

To: The Management of Compaya A/S
Compaya A/S Customers

Scope

We have been engaged to report on Compaya A/S (the Data Processor) description in section 3 of Compayas SMS-systems (CPSMS.dk, ProSMS.se/SMS.dk) and Compaya A/S and the related technical and organisational measures and other controls, relating to 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 with regard to the processing of personal data and on the free movement of such data (the EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions to the Regulation (Danish Data Protection Act), and on the design of the technical and organisational measures and other controls related to the control objectives stated in the description at 15 May 2023.

We have not performed procedures regarding the operating effectiveness of the controls stated in the description, and accordingly, we do not express an opinion on this.

The Data Processor's Responsibilities

The Data Processor is responsible for preparing the statement in section 2 and the accompanying description, including the completeness, accuracy, and method of presenting the statement and the description. Furthermore, the Data Processor is 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's Independence and Quality Control

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

BDO Statsautoriseret revisionsaktieselskab applies International Standard on Quality Management, 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 the Data Processor's description in section 3 and on the design of the controls related to the control objectives stated in the description, based on our procedures.

We conducted our engagement in accordance with the International Standard on Assurance Engagements 3000, "Reports Other Than Audits or Reviews of Historical Financial Information". That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are appropriately designed.

An assurance engagement to report on the description and design of controls at a Data Processor involves performing procedures to obtain evidence about the disclosures in the Data Processor's description, and about the design of the controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that controls are not appropriately designed. An assurance engagement of this type also includes evaluating the overall presentation of the description, the appropriateness of the objectives stated therein, and the suitability of the criteria specified by the Data Processor and described in section 2.

As described above, we have not performed procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, we do not express an opinion on this.

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

Limitations of Controls at a Data Processor

The Data Processor'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 use of Compayas SMS systems (CPSMS.dk, ProSMS.se/SMS.dk) and Compaya A/S and Compaya A/S that each individual Data Controller may consider important in their own environment. Also, because of their nature, controls with a Data Processor may not prevent or detect all breaches of the personal data security.

Opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the Data Processor's statement in section 2. In our opinion, in all material respects:

- a. The description presents fairly Compayas SMS systems (CPSMS.dk, ProSMS.se/SMS.dk) and Compaya A/S and the related technical and organisational measures and other controls, relating to processing and protection of personal data in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act, as designed and implemented per 15 May 2023.
- b. The technical and organisational measures and other controls, relating to the control objectives stated in the description were appropriately designed at 15 May 2023.

Description of Test of Controls

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


Intended Users and Purpose

This report is intended solely for data controllers, who have used Compaya's SMS systems (CPSMS.dk, ProSMS.se/SMS.dk) and Compaya A/S, and who have a sufficient understanding to consider it, along with other information, including information about the technical and organisational measures and other controls, operated by the data controllers themselves, when assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

Copenhagen, 26 May 2023

BDO Statsautoriseret Revisionsaktieselskab


Nicolai T. Visti
State Authorised Public Accountant


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

2. COMPAYA A/S' STATEMENT

Compaya A/S processes personal data in relation to Compaya's SMS systems (CPSMS.dk, ProSMS.se/SMS.dk) and Compaya A/S to our customers, who are Data Controllers according to 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 EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions (the Danish Data Protection Act).

The description has been prepared for Data Controllers who have used Compaya's SMS systems (CPSMS.dk, ProSMS.se/SMS.dk) and Compaya A/S, and who have a sufficient understanding to consider the description along with other information, including information about the technical and organisational measures and other controls operated by the Data Controllers themselves, in assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

Compaya A/S uses sub-processors. The sub-processor's relevant control objectives and related technical and organisational measures and other controls are not included in the accompanying description.

Compaya A/S confirms that the accompanying description in section 3 fairly presents Compaya's SMS systems (CPSMS.dk, ProSMS.se/SMS.dk) and Compaya A/S, which has processed personal data for the Data Controllers subject to the EU General Data Protection Regulation, and the related technical and organisational measures (controls) at 15 May 2023. The criteria used in making this statement were that we:

1. Present how Compaya's SMS systems (CPSMS.dk, ProSMS.se/SMS.dk) and Compaya A/S and the related technical and organisational measures and other controls were implemented, including:
 - The types of services provided, including the type of personal data processed.
 - The processes in both IT systems and business procedures applied to process personal data and, if necessary, correct and delete personal data as well as limiting the processing of personal data.
 - The procedures used to ensure that data processing has taken place in accordance with contract, instructions, or agreement with the data controller.
 - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality.
 - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation.
 - The procedures supporting in the event of breach of personal data security that the data controller may report this to the supervisory authority and inform the data subjects.
 - The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed.
 - The controls that we, with reference to the delimitation of Compaya's SMS systems (CPSMS.dk, ProSMS.se/SMS.dk) and would have been 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 are relevant to the processing of personal data.

2. Does not omit or distort information relevant to the scope of Compaya's SMS systems (CPSMS.dk, ProSMS.se/SMS.dk) and Compaya A/S and the related technical and organisational measures and other controls described while acknowledging that this description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Compaya's SMS systems (CPSMS.dk, ProSMS.se/SMS.dk) and Compaya A/S that the individual data controllers might consider important in their environment.

Compaya A/S confirms that the technical and organisational measures and other controls related to the control objectives stated in the accompanying description were suitable designed at 15 May 2023. The criteria we used in making this statement were that:

1. The risks threatening achievement of the described control objectives were identified.
2. The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

Compaya A/S confirms that appropriate technical and organisational measures and other controls were implemented and maintained to comply with the agreements with data controllers, good practices for the data processing of data and relevant requirements for Data Processors in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act.

Copenhagen, 26 May 2023

Compaya A/S



Martin Salder Schrøder
Executive/Partner

3. COMPAYA A/S' DESCRIPTION OF THE SMS-SYSTEMS

COMPAYA A/S

Compaya A/S is a Danish-owned company developing and operating the online services CPSMS.dk, ProSMS.se/SMS.dk for companies, unions, and public institutions etc. Compaya's office is located in Copenhagen.

Approximately 8 of Compaya's employees are specialised within sales and marketing, system development, server operation, support, and information security, and are organised in a sales department and development department.

The IT security officer controls Compaya's security of personal data in relation to the processing that Compaya handles on behalf of their clients, including entering into data processing agreements, replying to inquiries from the controller, communication of personal data breaches, compliance with internal policies and procedures, etc.

SMS SYSTEMS AND PROCESSING OF PERSONAL DATA

Compaya provides SMS systems as Software-as-a-Service (SaaS) solutions. To use the SMS systems, customers must accept the terms and conditions stated on the websites of the respective systems. In some cases, customers want a specific master agreement, which is made on request. Through the websites and in the SMS systems, we encourage customers to enter into a data processing agreement and prepare this electronically or, if necessary, send Compaya's standard data processing agreement adapted to the individual customer.

The SMS systems are developed at the office in Copenhagen, but are run from external hosting centres, which are sub-processors. Compaya has entered into a data processing agreement with these sub-processors.

In connection with the use of SMS systems by the controllers, Compaya collects and processes personal data about the controller. This data includes company name, address, name, e-mail, telephone number, CVR number and, if applicable, EAN number and log of activity using the SMS systems. These are only general personal data.

In the SMS systems, the controllers' users provide personal data about recipients of SMS messages. This is specifically the mobile number and possibly name. Controllers may also have entered personal data in the text field of the SMS message itself.

By default, Compaya processes data in the form of storing and transmitting the SMS messages that controllers have inserted into the SMS systems. A log of the sent text messages is stored, and the employees of Compaya have access to the information in these text messages via the user roles set up as system access. This access is used in connection with solving problems for controllers.

MANAGEMENT OF THE SECURITY OF PERSONAL DATA

Compaya has prepared requirements for establishing, implementing, maintaining and improving a management system for the security of personal data, which ensure compliance with the concluded agreements with the controllers, good data processor practice, and relevant requirements for Processors in accordance with the General Data Protection Regulation and the Danish Data Protection Act.

The technical and organisational security measures and other controls for protection of personal data are designed in accordance with the risk assessments and implemented to ensure confidentiality, integrity, and accessibility together with compliance with current data protection legislation. Security measures and controls are wherever possible automated and technically supported by IT systems.

Management of the security of personal data and the technical and organisation security measures and other controls are structured in the following key areas, for which control objectives and control activities have been defined:

ARTICLE	AREA
Article 28 (1)	The Processor's guarantees
Article 28 (3)	Data processing agreement
Article 28 (3)(a)(h) and (10) Article 29 Article 32 (4)	Instruction for processing of personal data
Article 28 (2) and (4)	Sub-processors
Article 28 (3)(b)	Confidentiality and professional secrecy
Article 28 (3)(c)	Technical and organisational 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)(h)	Assistance to the Controller
Article 30 (2) (3) (4)	Records of processing activities
Article 33 (2)	Communication of personal data breach.

RISK ASSESSMENT

It is Management's responsibility to take initiatives to address the threat scenario that Compaya is facing at all times, so that the security measures and controls introduced are appropriate, and the risk personal data breach, is reduced to a proper level.

The appropriate level of security is assessed on a current basis. The assessment takes into consideration risks relating to the accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.

An annual risk assessment is performed as the basis of updating of the technical and organisational security measures and other controls. The risk assessment illustrates the probability and consequences of incidents that may threaten the security of personal data and thereby natural persons' rights and freedoms, including incidental, intentional, and unintentional events. The risk assessment considers the actual technical level and implementation costs. As part of the risk assessment, an impact assessment (DPIA) has been carried out 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 organisational security measures and other controls concern all processes and systems, which process personal data on behalf of the Controller. The control objectives and control activities stated in the control schedule are an integral part of the subsequent description.

The Processor's guarantees

Compaya has introduced policies and procedures ensuring that Compaya can provide the sufficient guarantees for completing appropriate technical and organisational security measures in such a way that the processing complies with the requirements of the General Data Protection Regulation and ensures protection of the data subject's rights. Compaya has established an organisation of the security of personal data as

well as prepared and implemented an information security policy approved by Management, which is reviewed and updated on an ongoing basis.

Procedures for recruiting and resignation of employees as well as guidelines for training and instruction of employees processing personal data, including completion of awareness and information campaigns, exist.

Data processing agreement

Compaya has established a procedure for entering data processing agreements, specifying the conditions for processing personal data on behalf of the controller. Compaya applies the Danish Data Protection Agency's (Datatilsynet) template for data processing agreements in accordance with the services to be provided, including information on the use of subprocessors. The data processing agreements are digitally signed and stored electronically.

Compaya, as a processor, only carries out the processing of personal data on documented instructions from the controller, either in the data processing Agreement or in some cases following a separate instruction prepared by the controller.

As a processor, Compaya shall immediately inform the controller if an instruction in accordance with Compaya's opinion conflicts with the General Data Protection Regulation or data protection provisions of other EU law or national law of the Member States.

Subprocessors

The processor has the general approval of the controller to make use of subprocessors. However, the processor shall obtain the approval of the controller of any planned changes concerning the addition or replacement of other subprocessors and thereby give the controller the opportunity to object to such changes.

Compaya only uses subprocessors for server hosting in connection with the operation of the SMS systems.

Each year, typically in March, subprocessor must send a statement from an approved audit firm regarding the implementation of its own guidelines by subprocessors and their adequacy.

Confidentiality and professional secrecy

As a processor, Compaya ensures that only persons currently authorised to do so have access to the personal data processed on behalf of the Controller. Therefore, access to the data will be closed immediately if the authorisation is revoked or expired.

Only persons for whom it is necessary to have access to the personal data in order to fulfil the obligations of the Processor toward the controller may be authorised.

As a processor, Compaya ensures that the persons authorised to process personal data on behalf of the Controller have committed to confidentiality or are subject to an appropriate statutory obligation of confidentiality.

As a processor, Compaya can, at the request of the controller, demonstrate that the relevant employees are subject to the above-mentioned confidentiality.

Technical and organisational security measures

Risk Assessment

Compaya has completed the technical and organisational security measures since an assessment of risk in connection to confidentiality, integrity, and availability. Please refer to separate section about this.

Contingency plans

Compaya has established contingency plans so that Compaya can re-establish the availability of and access to personal data in due time in case of physical and technical events. Compaya has established a crisis response which takes effect in these cases. The arrangement of a crisis response group is established and guidelines for activation of the crisis response has been introduced.

Compaya has designed detailed contingency plans and plans for re-establishment of systems and data. The plans are available through Dropbox. The plans are tested and audited on an ongoing basis in connection with changes in systems etc.

Storage of personal data

Compaya has procedures in place to ensure that the storage of personal data is only carried out in accordance with Compaya's personal data policy. Access to personal data is granted based on work-related needs/need-to-know principles.

Physical access control

Compaya has introduced procedures ensuring that rooms are protected against unauthorised access. Compaya does not have secure rooms (server rooms etc.) and therefore, does not have access control with key cards, etc. Customers, suppliers, and other visitors are accompanied. Outside normal working hours, a code is required to the alarm system before you can enter the premises.

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

Logical access security

Compaya has established controls ensuring that access to systems and data are protected against unauthorised access to personal data. A user is created with unique user identification and password, and user identification is used by assigning access to resources and systems. All allocation of rights in systems is based on a work-related need. An assessment of the users' continued work-related need for access is reviewed at least once annually, including relevancy and correctness of allocated user rights. Procedures and controls support the process of creating, changing, and terminating users and allocated rights as well as review hereof.

The design of rules to length and complexity of password and termination of the user account after unsuccessful log-on attempts follows the best practice for a secure logical access control. Technical measures have been established to support these rules.

Remote workplaces and remote access to systems and data

Compaya has implemented procedures ensuring that access from workplaces outside Compaya premises and remote access to systems and data take place through VPN connections. Compaya has implemented procedures to ensure that external communication connections are secured with encryption.

Network security

Compaya has introduced procedures ensuring that networks in relation to application and security. Compaya's network for operation is located at team.blue Denmark A/S (Zitcom/Curanet/Wannafind) and at Rackhosting ApS and is separated from Compaya's office network. Access between the networks is restricted as far as possible, and access is controlled, as stated above. At Compaya's premises in Palægade, there is only network equipment to the office network, which is divided into VLAN's.

The office network at Compaya at the address in Palægade 4 is protected by the firewall, which is in our router, where all incoming traffic is generally closed, and open to all outgoing traffic. Some PCs and laptops are protected by the software firewall in Bitdefender Endpoint Security.

Anti-virus program and system updates

Compaya has introduced procedures ensuring that units with access to networks and applications are protected against virus and malware. Antivirus programmes and other protective systems are continually updated and adjusted in relation to the actual threat level.

Compaya has introduced procedures to ensure that system software is updated continuously following the suppliers' recommendations and recommendations. Patch Management procedures include operating systems, critical services, and relevant software installed on servers and workstations.

Back-up and re-establishment of data

Compaya has introduced procedures ensuring that systems and data are backed up to prevent loss of data or loss of accessibility in the event of critical failures. Back-ups are stored at an alternative location. A restore test of backup is performed continuously, but at least once a year.

Logging in systems, databases, and network

Compaya has introduced procedures ensuring that logging is set up in accordance with legislative requirements and business needs, based on a risk assessment of systems and the actual threat level. The scope and quality of log data are sufficient to identify and show possible abuse of systems or data, and log data is examined continually for applicability and abnormal conduct. Log data is secured.

Monitoring

Compaya has introduced procedures ensuring that ongoing monitoring of systems and introduced technical security measures.

Disposal of IT equipment

Storage media to be destroyed may be handed over to the IT security officer, who shall ensure an effective and permanent destruction of the media or data inside.

Data protection by design and by default

Compaya has implemented policies and procedures for developing and maintaining the SMS systems that ensure a managed change process. A change management procedure is used to manage development and change tasks, and each task follows the same process.

The development, test and production environment are separate, and every development or change task goes through a test process. Procedures have been introduced for version control, logging, and backup so that it is possible to reinstall previous versions.

Deletion and return of personal data

Compaya has introduced policies and procedures ensuring that personal data are deleted in accordance with instruction from the controller when the processing of personal data terminates at the end of contract with the controller.

Assistance to the controller

Compaya has introduced policies and procedures ensuring that Compaya can assist the controller in complying with their obligation to reply to requests on executing the data subjects' rights.

Compaya has introduced policies and procedures ensuring that Compaya can assist the controller in ensuring compliance with the obligations of article 32 on security of processing, article 33 on notification and communication of personal data breach, and article 34 - 36 on data protection impact assessment.

Compaya has introduced policies and procedures ensuring that Compaya can provide to the Controller all information necessary to demonstrate compliance with the requirements of the processors. Besides, Compaya allows and assists in audits, including inspections performed by the controller or others, who are authorised to do this by the controller.

Records of processing activities

Compaya has introduced policies and procedures ensuring that a record is kept of categories of processing activities that are performed on behalf of the controller. The record is updated regularly and controlled during the annual review of policies and procedures, etc. The record is stored electronically and can be provided for the supervisory authority, by request.

Communication of personal data breach

Compaya has introduced policies and procedures ensuring that personal data breaches are registered with detailed information about the event and that the controller is informed without undue delay after Compaya becomes aware of the personal data breach.

The registered information makes the controller able to assess whether the personal data breach must be reported to the supervisory authority and whether the data subjects should be notified.

COMPLEMENTARY CONTROLS WITH THE CONTROLLER

As part of the provision of the services, there are controls which are assumed to be implemented by the controllers and which are essential to achieving the control objectives set out in the description.

The controller has, inter alia, the following obligations:

- Ensuring that the instructions in the data processing agreement are legal in relation to the personal data law regulation in force at any time.
- Ensuring that the instructions in the agreed data processing agreement are appropriate in relation to the main service.
- The responsibility to ensure that the administrators use of the SMS systems and the processing of personal data are carried out in the systems are in accordance with data protection legislation.
- Ensuring that any special requirements for security measures at the controller are stated in the data processing agreement entered.
- Ensuring that the Controller's users in the SMS systems are up to date.

4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND THE RESULT OF TESTS

Objective and scope

We conducted our engagement in accordance with ISAE 3000, Assurance Reports Other Than Audits or Reviews of Historical Financial Information.

BDO has inspected procedures to obtain evidence of the information in Compaya A/S' description of the SMS systems and the design of the relating technical and organisational measures and other controls. The procedures selected depend on BDO's assessment, including the assessment of the risks that the description is not fairly presented and that the controls are not appropriately designed.

BDO's test of the design of the relating technical and organisational measures and other controls and their implementation has included the control objectives and related the control objectives and related control activities selected by Compaya A/S, and which are described in the check form below.

In the test form, BDO has described the tests carried out which were assessed necessary to obtain reasonable assurance that the stated control objectives were achieved, and that related controls were appropriately designed and operated effectively on 15. may 2023.

Test procedures

Test of the design of the relating technical and organisational measures and other controls and their implementation was performed by inquiries, inspection, and observation.

Type	Description
Inquiry	Inquiries of relevant personnel have been performed for all significant control activities. The purpose of the inquiries was to obtain knowledge and further information about implemented policies and procedures, including how the control activities are performed, and to obtain confirmed evidence of policies, procedures and controls.
Inspection	Documents and reports, which include information about the performance of the control, have been read for the purpose of assessing the design and monitoring of the specific controls, i.e., whether the design of the controls is such that they are expected to be effective if implemented, and whether the controls are sufficiently monitored and checked at suitable intervals. Tests have been performed of significant system structures of technical platforms, databases and network equipment to ensure that controls have been implemented, including for example assessment of logging, back-up, patch management, authorisations 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 control has been implemented.

For the services provided by Rackhosting ApS within hosting services, we have received an ISAE 3000 statement about the information security and measures for the period 1 May 2021 to 30 April 2022 according to the data processing agreement.

For the services provided by team.blue Denmark A/S (Zitcom/Curanet/Wannafind) within hosting services, we have received an ISAE 3402 statement about the information technical general controls related to the hosting services for the period 1. January to 31. December 2022.

These subprocessors' relevant control objectives and related controls are not included in Compaya A/S' description of the SMS systems and the technical and organisational security measures and other controls. Thus, we have solely assessed the received documentation and tested the controls at Compaya A/S, which ensures appropriate supervision of the subprocessor's compliance with the data processing agreement entered between the subprocessor and the processor and compliance with the General Data Protection Regulation and the Data Protection Act.

Result of test

The result of the test made of technical and organisational measures and other controls has resulted in the following exceptions noted.

An exception exists when:

- Technical and organisational measures and other controls have not been designed or implemented to fulfil a control objective, and
- Technical and organisational measures and other controls related to a control objective are not suitably designed and implemented.

Article 28 (1): The Processor's guarantees		
Control objectives ▶ To ensure that the Processor can provide the sufficient guarantees for protection of the Controller's personal data in accordance with the requirements of the General Data Protection Regulation and the protection of the data subject's rights.		
Control activities	Test performed by BDO	Result of test
Information security policy and data protection policy ▶ Compaya has prepared and implemented an information security policy. ▶ Compaya has prepared and implemented a data protection policy.	We have interviewed relevant personnel at Compaya. We inspected Compaya's information security policy. We inspected Compaya's protection policy for Compaya's SMS systems (CPSMS.dk, ProSMS.se/SMS.dk)	No exceptions noted.
Review of the information security policy and data protection policy ▶ Compaya's information security policy and data protection policy are reviewed and updated at least once annually. ▶ An IT-security committee has been established to review and approve the information security policy and the IT security handbook.	We have interviewed relevant personnel at Compaya. We observed that an annual cycle of work has been prepared, which helps to ensure that the information security policy and data protection policy are reviewed and updated at least once annually. We observed that Compaya's information security policy was approved by Management in August 2022, and that an assessment of the need for updating the data protection policy was made, after which the data protection policy for ProSMS.se/SMS.dk and CPSMS was last updated in September 2022. We observed that an IT security committee is established. We have carried out an inspection of documentation, which confirms that the IT security committee reviews and approves the information security policy and the related IT security handbook.	No exceptions noted.

Article 28 (1): The Processor's guarantees		
Control objectives ▶ To ensure that the Processor can provide the sufficient guarantees for protection of the Controller's personal data in accordance with the requirements of the General Data Protection Regulation and the protection of the data subject's rights.		
Control activities	Test performed by BDO	Result of test
Recruitment of employees ▶ Compaya has prepared and implemented a procedure for recruiting new employees, including screening of employees before recruitment.	We have interviewed relevant personnel at Compaya. We inspected the procedure for recruiting new employees. On inquiry, we were informed that no new employees have been employed in the past year, so it has not been possible to test the implementation of the introduced control.	No exceptions noted.
Resignation of employees ▶ Compaya has prepared and implemented a procedure for the resignation of employees upon termination of employment. Management must ensure that the procedure is followed and documented.	We have interviewed relevant personnel at Compaya. We inspected the procedure for resignation of employees upon termination of employment. On inquiry, we were informed that no employees have resigned in the past year, so it has not been possible to test the implementation of the introduced control.	No exceptions noted.
Education, awareness, and information campaigns for employees ▶ Compaya ensures that employees are informed about the procedures and politics regarding the treatment of personal data. ▶ Compaya continually conducts awareness campaigns in the form of notices, meetings, and e-mails etc.	We have interviewed relevant personnel at Compaya. We inspected the IT security handbook. We inspected the procedure for training of employees and observed that there are provisions stating that employees shall have knowledge about the information security policy and the IT-security handbook, and provisions about treatment of personal data.	No exceptions noted.

Article 28 (1): The Processor's guarantees**Control objectives**

- ▶ *To ensure that the Processor can provide the sufficient guarantees for protection of the Controller's personal data in accordance with the requirements of the General Data Protection Regulation and the protection of the data subject's rights.*

Control activities	Test performed by BDO	Result of test
	We have carried out an inspection of documentations, which confirms that Compaya continually performs awareness campaigns in the forms of online courses and e-mails etc.	

Article 28 (3): Data processor agreement		
Control objectives		
<p>▶ To ensure that the Data Processor enters a written contract with the Controller, who determines the terms for the processing of the Controller's personal data, and that the contract is stored electronically.</p>		
Control activities	Test performed by BDO	Result of test
<p>Entering into a data processor agreement with the Controller</p> <ul style="list-style-type: none"> ▶ Compaya has a procedure for entering a written data processing agreement, which is in accordance with the services delivered by the data processor. ▶ Compaya applies a template when entering data processing agreements. ▶ Data processing agreements are signed and stored electronically. ▶ Data processing agreements contains information about the use of subprocessors. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We inspected the procedure when entering a written data processing agreement, which is in accordance with the services delivered by Compaya.</p> <p>We observed that Compaya has prepared a template when entering a data processing agreement. It is our assessment that the template completes the requirements of the General Data Protection Regulation article 28 (3).</p> <p>We have carried out an inspection of documentation, which confirms that the data processing agreements are signed and stored electronically.</p> <p>We inspected an entered data processing agreement for CPSMS.dk and ProSMS.se/SMS.dk, respectively, and observed that the data processing agreement includes information about the use of subprocessors.</p>	<p>No exceptions noted.</p>

Article 28 (3) and (10), article 29 and article 32 (4): Instruction for processing of personal data		
Control objectives <ul style="list-style-type: none"> ▶ To ensure that the Data Processor solely acts on documented instruction by the Controller. ▶ To ensure that the Data Processor communicates to the Controller, if an instruction is in contravention of the General Data Protection Regulation and the data protection legislation. 		
Control activities	Test performed by BDO	Result of test
Instruction for processing of personal data <ul style="list-style-type: none"> ▶ Compaya ensures, that entered data processing agreement contains instructions from the controllers. ▶ Compaya only processes personal data as stated in the instructions from the controller. ▶ Compaya has prepared and implemented written procedures regarding the processing of personal data, so that processing is only carried out in accordance with instructions from the controller. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We observed that an agreement template has been prepared when entering into data processing agreements.</p> <p>We have inspected Compaya's procedure regarding the processing of personal data and observed that it states that the personal data must be processed in accordance with instructions from the Controller.</p> <p>We inspected one sample of entered data processing agreements for CPSMS.dk and ProSMS.se/SMS.dk, respectively, and observed that the data processing agreements contain an instruction from the Controllers.</p>	No exceptions noted.
Notification of the Controller in case of unlawful instruction <ul style="list-style-type: none"> ▶ The data processing agreement contains terms that the Controller must be informed about instructions that are contrary to legislation. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We observed that an agreement template has been prepared when entering into data processing agreements.</p> <p>We inspected one sample for entered data processing agreements for CPSMS.dk and ProSMS.se/SMS.dk, respectively, and observed that the data processing agreements include terms that the Controller must be informed about instructions that are contrary to legislation.</p> <p>On inquiry, we were informed that there have not been examples of data processing agreements that have been contrary to legislation, for which reason it has not been possible to test the control introduced.</p>	No exceptions noted.

Article 28 (2) and (4): Subprocessors		
<p>Control objectives</p> <ul style="list-style-type: none"> ▶ To ensure that the subprocessor has been assigned the same data protection obligations as the Data Processor is assigned by the Controller, by entering into a written contract with relating instruction. ▶ To ensure that the Controller has given their preceding specific or general written approval of subprocessors. ▶ To ensure that the subprocessor can provide the sufficient guarantees for protection of personal data in accordance with the contract. 		
Control activities	Test performed by BDO	Result of test
<p>Sub data processing agreement and instruction</p> <ul style="list-style-type: none"> ▶ When using subprocessors, Compaya enters a sub data processing agreement, which assigns the same data protection obligations to the subprocessor as those assigned to the Data Processor. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We inspected the procedure for managing data processors.</p> <p>We inspected one sub data processing agreement and observed that it contains the same data protection obligations, which are imposed on Compaya.</p>	<p>No exceptions noted.</p>
<p>Approval of subprocessors</p> <ul style="list-style-type: none"> ▶ Replacement of subprocessors follows the prior approval process entered into with the Controller. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We observed that an agreement template has been prepared when entering into data processing agreements and a procedure for managing these agreements.</p> <p>We inspected one sample of data processing agreements for CPSMS.dk and ProSMS.se/SMS.dk, respectively, and observed that the data processing agreements contain provisions regarding the replacement of subprocessors.</p> <p>On inquiry, we were informed that in the last year there has been no cases where the data processor has made changes in relation to approved subprocessors, for which reason it has not been possible to test the implementation of the control introduced.</p>	<p>No exceptions noted.</p>

Article 28 (2) and (4): Subprocessors

Control objectives

- ▶ To ensure that the subprocessor has been assigned the same data protection obligations as the Data Processor is assigned by the Controller, by entering into a written contract with relating instruction.
- ▶ To ensure that the Controller has given their preceding specific or general written approval of subprocessors.
- ▶ To ensure that the subprocessor can provide the sufficient guarantees for protection of personal data in accordance with the contract.

Control activities	Test performed by BDO	Result of test
<p>Supervision of sub data processors</p> <ul style="list-style-type: none"> ▶ Compaya conducts supervision, including obtains and reviews the subprocessor's audit opinions, certifications, and similar documents etc. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We inspected the procedure for managing subprocessors and observed that there are provisions regarding the collection and review of auditors' statements, certifications, and similar documents of the sub data processors.</p> <p>We have carried out an inspection of documentation confirming that a review of declarations obtained from the subprocessors has been carried out. On inquiry, we were informed that an ISAE 3402 from team.blue Denmark has been found sufficient, since it is only about hosting.</p> <p>We inspected the ISAE 3402 declaration from team.blue Denmark A/S for the period 1 January to 31 December 2022 and ISAE 3000 from Rackhosting ApS for the period 1 May 2021 - 30 April 2022.</p>	<p>No exceptions noted.</p>

Article 28 (3)(b): Confidentiality and professional secrecy

Control objectives

- ▶ To ensure that the staff authorised to process personal data have accepted an obligation of confidentiality or are subject to an appropriate professional secrecy.

Control activities	Test performed by BDO	Result of test
<p>Confidentiality and secrecy agreement with employees</p> <ul style="list-style-type: none"> ▶ All employees have signed an employment contract, which contains a section regarding confidentiality. ▶ Compaya enters into confidentiality agreements with external consultants with access to personal data. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We inspected the procedure when entering a confidentiality and secrecy agreement with employees.</p> <p>We inspected one sample for an employee and observed that the employee has signed the employment contract, and it contains a provision about confidentiality and secrecy agreement.</p> <p>We inspected one sample for a consultant and observed that the consultant has signed the confidentiality agreement.</p>	<p>No exceptions noted.</p>

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- ▶ To ensure that the Data Processor has implemented appropriate technical and organisational security measures in consideration of the actual technical level, the implementation costs and the nature of the relevant processing, scope, correlation, and purpose as well as the risks of varying likelihood and gravity for people's rights and freedoms (risk assessment), including an ongoing review and updating of risk assessment and security measures.
- ▶ To ensure that the risk assessment takes into consideration risks relating to the accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.
- ▶ To ensure confidentiality, integrity and accessibility robustness of processing systems and services.
- ▶ To ensure timely re-establishment of the accessibility of and access to personal data in case of a physical or technical event.
- ▶ To ensure regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures for ensuring the security of processing.

Control activities	Test performed by BDO	Result of test
Risk Assessment <ul style="list-style-type: none"> ▶ Compaya has prepared a risk assessment in relation to the registered rights and freedoms rights. ▶ Compaya has developed and implemented a procedure to ensure that the safety measures are reviewed and updated. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We inspected the risk assessment and observed, that an assessment has been made about the risks and consequences in relation to the General Data Protection Regulation.</p> <p>We inspected the annual cycle of work, which ensures continuous assessment and updates on the security measures, and we observed that a half yearly update on the risk assessment has been made.</p>	No exceptions noted.
Contingency plans in case of physical or technical incidents <ul style="list-style-type: none"> ▶ Compaya has prepared a contingency plan. ▶ Compaya has carried out a test of the contingency plan. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We inspected the contingency plan and observed that the contingency plan includes a description of, among other things, role and responsibility in the contingency organisation, prerequisites for activation and plan for escalation.</p> <p>We inspected the IT contingency plan and observed that it was last updated in February 2022.</p> <p>We inspected documentation for consistent desk checking of the IT contingency plan as well as experience gathering.</p>	No exceptions noted.

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- ▶ To ensure that the Data Processor has implemented appropriate technical and organisational security measures in consideration of the actual technical level, the implementation costs and the nature of the relevant processing, scope, correlation, and purpose as well as the risks of varying likelihood and gravity for people's rights and freedoms (risk assessment), including an ongoing review and updating of risk assessment and security measures.
- ▶ To ensure that the risk assessment takes into consideration risks relating to the accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.
- ▶ To ensure confidentiality, integrity and accessibility robustness of processing systems and services.
- ▶ To ensure timely re-establishment of the accessibility of and access to personal data in case of a physical or technical event.
- ▶ To ensure regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures for ensuring the security of processing.

Control activities	Test performed by BDO	Result of test
	On inquiry, we were informed that the test of the IT-contingency plan did not lead to any changes of the IT contingency plan.	
Storage of personal data <ul style="list-style-type: none"> ▶ Personal data in electronic form are only available for the data processor's employees. ▶ Access to personal data is assigned based on the work-related needs/need-to-know principles. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We inspected the IT security handbook and procedure for accessing personal data. We have carried out an inspection of documentation confirming only authorised employees have access to personal information.</p> <p>We inspected the procedure for access to personal data and observed that it states that access to personal data is granted based on work-related needs/need-to-know principles.</p>	No exceptions noted.
Physical access control <ul style="list-style-type: none"> ▶ Physical access control is established regarding Compaya's office and premises. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We inspected the IT security handbook and observed that a procedure describes the physical access control in relation to the data processors offices and premises.</p> <p>We inspected the list of keys and pieces that have been handed over to employees in accordance with the data processor's procedure.</p>	No exceptions noted.

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- ▶ *To ensure that the Data Processor has implemented appropriate technical and organisational security measures in consideration of the actual technical level, the implementation costs and the nature of the relevant processing, scope, correlation, and purpose as well as the risks of varying likelihood and gravity for people's rights and freedoms (risk assessment), including an ongoing review and updating of risk assessment and security measures.*
- ▶ *To ensure that the risk assessment takes into consideration risks relating to the accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.*
- ▶ *To ensure confidentiality, integrity and accessibility robustness of processing systems and services.*
- ▶ *To ensure timely re-establishment of the accessibility of and access to personal data in case of a physical or technical event.*
- ▶ *To ensure regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures for ensuring the security of processing.*

Control activities	Test performed by BDO	Result of test
Logical access control <ul style="list-style-type: none"> ▶ Compaya has implemented a procedure for user administration procedure to ensure that user creation and termination follow a managed process, and that all user creations are authorised. ▶ Continuous review of users and user rights. ▶ Compaya's requirement for passwords is complied with by all employees as well as external consultants. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We have carried out an inspection of the user administration procedure and observed that there are guidelines for creating and terminating users.</p> <p>We have carried out an inspection of the IT security handbook and observed that according to it, at least once a year a review of users' rights must be carried out.</p> <p>We have carried out an inspection of documentation, which confirms that Compaya has reviewed users and user rights in May 2023, in accordance with the annual cycle of work.</p> <p>We have carried out an inspection of documentation, which confirms that password requirements are followed by all employees as well as external consultants.</p>	No exceptions noted.
Remote workplaces and remote access to systems and data <ul style="list-style-type: none"> ▶ Remote access to Compaya's systems and data is via an encrypted VPN connection. ▶ A secure connection is being used between Compaya and the subprocessor. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We have carried out an inspection of documentation, which confirms that a VPN connection with encryption.</p> <p>We have carried out an inspection of documentation, which confirms that there is a secure connection between Compaya and the subprocessor.</p>	No exceptions noted.

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- ▶ To ensure that the Data Processor has implemented appropriate technical and organisational security measures in consideration of the actual technical level, the implementation costs and the nature of the relevant processing, scope, correlation, and purpose as well as the risks of varying likelihood and gravity for people's rights and freedoms (risk assessment), including an ongoing review and updating of risk assessment and security measures.
- ▶ To ensure that the risk assessment takes into consideration risks relating to the accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.
- ▶ To ensure confidentiality, integrity and accessibility robustness of processing systems and services.
- ▶ To ensure timely re-establishment of the accessibility of and access to personal data in case of a physical or technical event.
- ▶ To ensure regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures for ensuring the security of processing.

Control activities	Test performed by BDO	Result of test
Network security <ul style="list-style-type: none"> ▶ Compaya's office network is segmented. ▶ Compaya uses known network technologies and mechanisms to monitor the office network. ▶ The number of employees with access to make changes in the firewall for the office network is limited. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We have carried out an inspection of documentation for network segmentation.</p> <p>We have carried out an inspection of documentation, which confirms that Zabbix is applied to monitor the office network.</p> <p>We have carried out an inspection of documentation, which confirms that only authorised employees have access to make changes in Compaya's local networks firewall.</p>	No exceptions noted.
Antivirus program and system updates <ul style="list-style-type: none"> ▶ Anti-virus software is installed on all workstations. ▶ The employees' PCs are programmed to update automatically (Patch Management). 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We inspected the data processor's procedure for protection against virus and malware etc.</p> <p>We have carried an inspection of one sample for documentation, that antivirus has been installed on an employee's PC. We observed that antivirus is activated.</p> <p>We have carried out an inspection of documentation, which confirms that the employees' PCs are automatically updated.</p>	No exceptions noted.

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- ▶ To ensure that the Data Processor has implemented appropriate technical and organisational security measures in consideration of the actual technical level, the implementation costs and the nature of the relevant processing, scope, correlation, and purpose as well as the risks of varying likelihood and gravity for people's rights and freedoms (risk assessment), including an ongoing review and updating of risk assessment and security measures.
- ▶ To ensure that the risk assessment takes into consideration risks relating to the accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.
- ▶ To ensure confidentiality, integrity and accessibility robustness of processing systems and services.
- ▶ To ensure timely re-establishment of the accessibility of and access to personal data in case of a physical or technical event.
- ▶ To ensure regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures for ensuring the security of processing.

Control activities	Test performed by BDO	Result of test
Back-up and re-establishment of data <ul style="list-style-type: none"> ▶ Compaya has prepared and implemented a procedure for back-up. ▶ Back-up of systems and data is performed daily. ▶ A restore test of backup is performed continuously, but at least once a year. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We inspected Compaya's back-up policy and procedure for back-up, as well as verification and re-establishment of back-up.</p> <p>We have carried out an inspection of documentation, which confirms that a daily back-up of systems and data is carried out.</p> <p>We inspected documentation for performed restore tests of back-ups carried out in December 2022.</p>	No exceptions noted.
Logging when use of personal information <ul style="list-style-type: none"> ▶ All successful and failed attempts to access the SMS-systems and data are logged. ▶ Logfiles are only available for the operating and support employees. ▶ Log data with personal data is deleted after 6 months. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We have carried out an inspection of documentation, which confirms that all successful and failed access attempts to the SMS systems (CPSMS.dk, ProSMS.se/SMS.dk) and data are logged.</p> <p>We have carried out an inspection of documentation, which confirms that logfiles are only available to the operating and support employees.</p>	No exceptions noted.

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- ▶ To ensure that the Data Processor has implemented appropriate technical and organisational security measures in consideration of the actual technical level, the implementation costs and the nature of the relevant processing, scope, correlation, and purpose as well as the risks of varying likelihood and gravity for people's rights and freedoms (risk assessment), including an ongoing review and updating of risk assessment and security measures.
- ▶ To ensure that the risk assessment takes into consideration risks relating to the accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.
- ▶ To ensure confidentiality, integrity and accessibility robustness of processing systems and services.
- ▶ To ensure timely re-establishment of the accessibility of and access to personal data in case of a physical or technical event.
- ▶ To ensure regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures for ensuring the security of processing.

Control activities	Test performed by BDO	Result of test
	We have carried out an inspection of documentation, which confirms that log data with personal data are deleted after 6 months.	
Monitoring <ul style="list-style-type: none"> ▶ Compaya has established a monitoring system to monitor the production environments, including uptime, performance, and capacity. ▶ Compaya is notified of identified alerts and follows up on these. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We inspected the IT security handbook, in which the procedure for monitoring is described.</p> <p>We have carried out an inspection of documentation regarding monitoring and observed that Zabbix is used to monitor the production environment, including uptime, performance, and capacity.</p> <p>We have carried out an inspection of documentation, which confirms that Compaya receives messages in the form of e-mails from Zabbix with identified alerts.</p>	No exceptions noted.
Guidelines for disposal or destruction of IT equipment <ul style="list-style-type: none"> ▶ Personal data are removed/overwritten in relation to PCs that are disposed of or recycled. ▶ Compaya disposes of IT equipment by physical destruction of data-bearing media. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We inspected the IT security handbook and observed that a procedure describes the repairment and disposal of IT equipment.</p>	No exceptions noted.

Article 28 (3)(c): Technical and organisational security measures

Control objectives

- ▶ *To ensure that the Data Processor has implemented appropriate technical and organisational security measures in consideration of the actual technical level, the implementation costs and the nature of the relevant processing, scope, correlation, and purpose as well as the risks of varying likelihood and gravity for people's rights and freedoms (risk assessment), including an ongoing review and updating of risk assessment and security measures.*
- ▶ *To ensure that the risk assessment takes into consideration risks relating to the accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure of or access to personal data, which is transmitted, stored, or otherwise processed.*
- ▶ *To ensure confidentiality, integrity and accessibility robustness of processing systems and services.*
- ▶ *To ensure timely re-establishment of the accessibility of and access to personal data in case of a physical or technical event.*
- ▶ *To ensure regular testing, assessment, and evaluation of the efficiency of the technical and organisational security measures for ensuring the security of processing.*

Control activities	Test performed by BDO	Result of test
	We were informed that there has not been a situation, where Compaya has had to dispose of IT equipment by physical destruction, which is why it has not been possible to test the implementation of the introduced controls.	

Article 25: Data protection by design and by default

Control objectives

- ▶ To ensure that the Data Processor completes data protection by design and by default.

Control activities	Test performed by BDO	Result of test
<p>Development and Maintenance of systems</p> <ul style="list-style-type: none"> ▶ Compaya has prepared a procedure for the development process, which ensures Privacy-by-Design and Privacy by Default. ▶ Compaya instructs the employees on Privacy by Design and Privacy by Default. ▶ Development and tests are carried out in development environments, which are separated from the production systems. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We inspected Compaya's procedure for the development process, which ensures data protection through design and standard settings.</p> <p>We have carried out an inspection of documentation, which confirms that Compaya has instructed the employees on the requirements to Privacy by Design and Privacy by Default.</p> <p>We inspected the network topology, which confirms that the development, test, and production environments are separated.</p> <p>We have carried out an inspection of documentation which shows that the continuous progress of development tasks is documented in Compaya's task management system Pivotal Tracker.</p>	<p>No exceptions noted.</p>

Article 28 (3)(g) - Deletion of personal data		
Control objectives ► To ensure that the Data Processor can delete and return personal data when the service regarding the processing has terminated, in accordance with instruction from the Controller.		
Control activities	Test performed by BDO	Result of test
Deletion of personal data ► Compaya deletes the Controller's personal data after instruction, by termination of the main agreement.	<p>We have interviewed relevant personnel at Compaya.</p> <p>We inspected the procedure for processing customer data and observed that a procedure for deleting personal data has been described.</p> <p>We have carried out an inspection of documentation which confirms that technical measures have been implemented to enable the deletion of personal data in the SMS systems (CPSMS.dk, ProSMS.se/SMS.dk).</p> <p>On inquiry, we were informed that there have been no inquiries from the Controller regarding the deletion of personal data, for which reason it has not been possible to test the implementation of the control introduced.</p>	No exceptions noted.

Article 28 (3)(e)(f)(h): Assistance to the Controller

Control objectives

- ▶ To ensure that the Data Processor can assist the Controller in fulfilling of the data subject's rights.
- ▶ To ensure that the Data Processor can assist the Controller in relation to security of processing (article 32), personal data breaches (article 33-34) and data protection impact assessments (article 35-36).
- ▶ To ensure that the Data Processor can assist the Controller in relation to audit and inspection.

Control activities	Test performed by BDO	Result of test
<p>Assistance - The data subjects' rights</p> <ul style="list-style-type: none"> ▶ Compaya can has assist the Controller in compliance with the data subjects' rights. ▶ Compaya provide insight into all information registered at the data processor. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We inspected the procedure for assistance to the Controller and observed that there are provisions regarding assistance in fulfilling the registered rights.</p> <p>We inspected the template for data processing agreement as well as one sample of a signed data processing agreement for CPSMS.dk, ProSMS.se/SMS.dk, respectively, and observed that it appears that the data processor must assist the Controller with compliance with the registered rights.</p> <p>On inquiry, we were informed that there has not been a case of handling assistance to the Controller, for which reason it has not been possible to test the implementation of the controls introduced.</p> <p>We observed that the data processor can provide insight into all information registered with the data processor.</p>	<p>No exceptions noted.</p>
<p>Assistance - Audit and inspection</p> <ul style="list-style-type: none"> ▶ Compaya annually prepares an ISAE 3000 assurance report about the technical and organisational security measures aimed towards processing and protection of personal information. ▶ Compaya assists the Controller at physical supervision. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We inspected the template for the data processing agreement and observed that it appears that the data processor must annually prepare an ISAE 3000 assurance report on the technical and organisation security measures aimed towards processing and protection of personal information.</p> <p>We have prepared this ISAE 3000 assurance report for the purpose of obligations of the processor in this relation.</p>	<p>No exceptions noted.</p>

Article 28 (3)(e)(f)(h): Assistance to the Controller		
<p>Control objectives</p> <ul style="list-style-type: none"> ▶ To ensure that the Data Processor can assist the Controller in fulfilling of the data subject's rights. ▶ To ensure that the Data Processor can assist the Controller in relation to security of processing (article 32), personal data breaches (article 33-34) and data protection impact assessments (article 35-36). ▶ To ensure that the Data Processor can assist the Controller in relation to audit and inspection. 		
Control activities	Test performed by BDO	Result of test
	<p>We inspected the procedure for assistance to the Controller and observed that provisions regarding assistance in relation to audit and inspection are included.</p> <p>We observed that the data processing agreement states that the data processor is committed to assist the Controller by physical supervision.</p> <p>On inquiry, we were informed that there has been no case of assistance with physical inspections, for which reason it has not been possible to test the implementation of the controls introduced.</p>	
<p>Assistance - special requirements in the regulation.</p> <ul style="list-style-type: none"> ▶ Compaya can assist the controller in relation to compliance with processing security (article 32), notification of personal data breaches to controllers (article 33), data protection impact assessment (article 35), prior consultation (article 36). 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We inspected the following documentation:</p> <ul style="list-style-type: none"> * Information security policy * Data protection policy for each of the SMS systems * Procedure for processing personal data breaches. * Data breach log of the data processor * Procedure for accessing personal data in the SMS systems. * Procedure for processing customer data in the SMS systems <p>We inspected the procedure for assistance to the Controller and observed that it states provisions in relation to compliance with the special requirements of the regulation, including notification of security breaches, impact assessments and prior consultations by the supervisory authorities.</p> <p>On inquiry, we were informed that there has been no case of assistance to the Controller regarding the special requirements in the regulation in accordance with Articles 32 to 36, for which</p>	<p>No exceptions noted.</p>

Article 28 (3)(e)(f)(h): Assistance to the Controller

Control objectives

- ▶ *To ensure that the Data Processor can assist the Controller in fulfilling of the data subject's rights.*
- ▶ *To ensure that the Data Processor can assist the Controller in relation to security of processing (article 32), personal data breaches (article 33-34) and data protection impact assessments (article 35-36).*
- ▶ *To ensure that the Data Processor can assist the Controller in relation to audit and inspection.*

Control activities	Test performed by BDO	Result of test
	reason it has not been possible to test the implementation of the introduced procedures.	

Article 30 (2) (3) (4): Records of processing activities		
Control objectives <ul style="list-style-type: none"> ▶ To ensure that the Data Processor prepares a written record of all categories of processing activities carried out on behalf of the Controller. ▶ To ensure that the Data Processor stores the written record electronically. ▶ To ensure that the Data Processor can make available the record to the supervisory authority. 		
Control activities	Test performed by BDO	Result of test
List of processing activities <ul style="list-style-type: none"> ▶ Compaya has established a record of processing activities as Data Processor. ▶ The record is kept electronically. ▶ The record is updated continually and at least once a year under the yearly review. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We observed that Compaya has compiled records of processing activities. We have inspected the processing activity.</p> <p>We observed that the record is kept electronically.</p> <p>We inspected the annual cycle of work and observed that an update of the record takes place continuously and at least once a year, which appears from the annual cycle of work.</p>	<p>No exceptions noted.</p>

Article 33 (2): Communication of personal data breach

Control objectives

- ▶ To ensure that the Data Processor without undue delay communicates to the Controller personal data breaches.
- ▶ To ensure that the Controllers are notified of all information necessary, so that the breach can be assessed for the purpose of reporting it to the supervisory authority and communicating it to the data subject.

Control activities	Test performed by BDO	Result of test
<p>Communication of personal data breach</p> <ul style="list-style-type: none"> ▶ Compaya has developed a procedure for handling personal data breaches. ▶ Compaya has prepared and implemented a procedure for notifying the Controller in the event of a personal data breach. ▶ Compaya registers personal data breaches in the data breach log. 	<p>We have interviewed relevant personnel at Compaya.</p> <p>We inspected the procedure for handling personal data breaches and observed that guidelines for registering personal data breaches have been described.</p> <p>We inspected the procedure for notifying the Controller in the event of a personal data breach and observed that it appears that the Controller must be informed without undue delay after Compaya has become aware of a personal data breach.</p> <p>We inspected the data breach log, which must be completed in case of a personal data breach.</p> <p>On inquiry, we were informed that there has been no personal data breach, for which reason it has not been possible to test the implementation of the introduced controls.</p>	<p>No exceptions noted.</p>

**BDO STATS AUTORISERET
REVISIONSAKTIESELSKAB**

HAVNEHOLMEN 29
1561 KØBENHAVN V

CVR NO. 20 22 26 70

BDO Statsautoriseret revisionsaktieselskab, a Danish limited liability company, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO in Denmark employs almost 1,400 people and the worldwide BDO network has more than 111,000 partners and staff in 164 countries.

Copyright - BDO Statsautoriseret revisionsaktieselskab, CVR No. 20 22 26 70.

