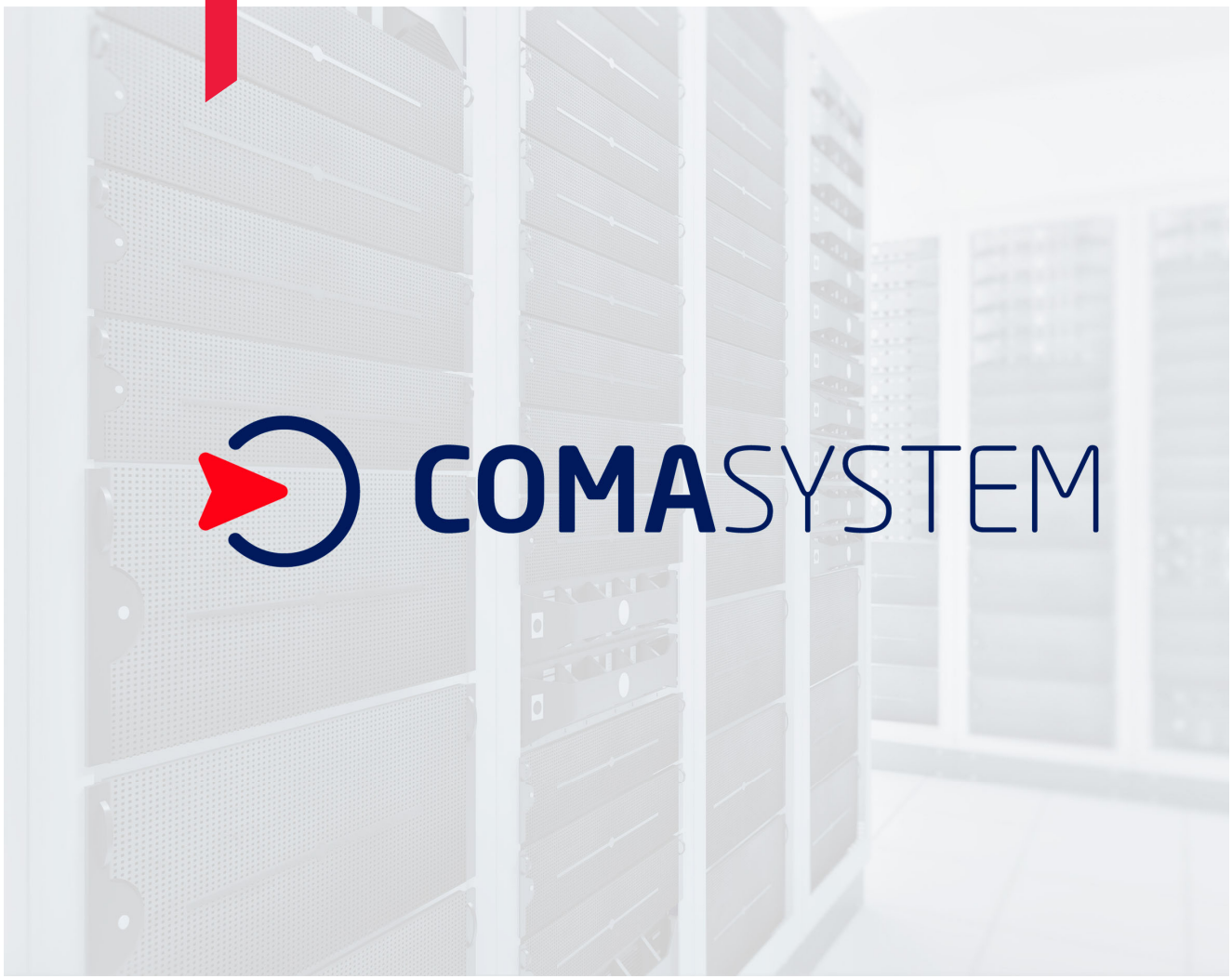

COMASYSTEM APS

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD 1 OCTOBER 2022 TO 30 SEPTEMBER 2023 ON THE DESCRIPTION OF COMASYSTEM AND RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS, RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH DATA PROTECTION ACT.

CONTENTS

1. INDEPENDENT AUDITOR'S REPORT

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD 1 OCTOBER 2022 TO 30 SEPTEMBER 2023 ON THE DESCRIPTION OF COMASYSTEM AND THE RELATED TECHNICAL AND ORGANISATIONAL SECURITY MEASURES AND OTHER CONTROLS, THEIR DESIGN AND OPERATING EFFECTIVENESS AIMED AT PROCESSING AND PROTECTION OF PERSONAL DATA UNDER THE GENERAL DATA PROTECTION REGULATION AND THE DANISH DATA PROTECTION ACT

To: The Management of COMAsystem ApS
COMAsystem ApS' customers (data controllers)

Scope

We have been engaged to report on COMAsystem ApS' (the data processor) description in section 3 of COMASYSTEM 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 and operating effectiveness of the technical and organisational measures and other controls related to the control objectives stated in the description for the period 1 October 2021 to 30 September 2022.

The data processor's responsibilities

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

Auditor's independence and quality control

We have complied with the requirements 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 and operating effectiveness of the controls related to the control objectives stated in the description, based on our procedures.

We have performed our work in accordance with ISAE 3000 on other assurance engagements with certainty than audit or review 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, design and operating effectiveness of controls at a Data Processor involves performing procedures to obtain evidence about the disclosures in the Data Processor's description and about the design and operating effectiveness 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 or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. In addition, an assurance engagement with certainty of this type includes assessment of the total presentation of the description, the appropriateness of the herein stated control objectives as well as the appropriateness of the criteria specified and described in section 2.

In our opinion, the evidence obtained is sufficient and suitable to form basis for our conclusion.

Limitations of controls with a data processor

The data processor's description is prepared to meet the common needs of a wide range of data controllers and therefore may not include all the aspects when applying COMASYSTEM that each individual data controller may consider important in their own special environment. Also, because of their nature, controls at a data processor may not prevent or detect all breaches of the personal data security. Furthermore, the projection of any evaluation of the operating effectiveness of controls to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Conclusion

Our opinion has been formed on the basis of matters outlined in this report. The criteria we used in forming our opinion are those described in the data processor's statement in section 2. In our opinion

a. the description of COMASYSTEM and the relating technical and organisational security measures and other controls related to processing and protection of personal data in accordance with the General Data Protection Regulation and the Data Protection Act as they were designed and implemented in the entire period from 1 October 2022 to 30 September 2023, in all material respects is fair, and

b. that the technical and organisational measures and other controls relating to the control objectives stated in the description in all material respects were suitably designed in the entire period from 1 October 2022 to 30 September 2023, and

c. that tested technical and organisational measures and other controls, which were the ones necessary for expressing a high degree of certainty that the control objectives in the description were reached in all material respects, have performed efficiently in the entire period from 1 October 2022 to 30 September 2023.

Description of test of controls

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

Intended users and objective

This internal report is intended solely for the data controllers, who have applied the data processor's COMASYSTEM, and who have sufficient understanding to assess this report together with other information, including the technical and organisational security measures and other controls performed by the data controllers themselves, when assessing whether the provisions of the General Data Protection Regulation and the Data Protection Act have been complied with.

Copenhagen, 24 October 2023

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, State-Authorised Public Accountant

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

2. COMASYSTEM APS' STATEMENT

COMAsystem ApS handles processing of personal data in connection with COMASYSTEM for our clients who are data controllers in accordance with the regulation of the European Parliament and of the Council on 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 Data Protection Act).

The accompanying description is prepared for the data controllers, who have applied COMASYSTEM, and who have sufficient understanding to assess the description together with other information, including the technical and organisational security measures and other controls performed by the data controllers themselves, when assessing whether the provisions of the General Data Protection Regulation and the Data Protection Act have been complied with.

COMAsystem ApS uses subprocessors. The subprocessors' relevant control objectives and relating technical and organisational security measures and other controls are not included in the following description.

COMAsystem ApS confirms that the accompanying description in section 3 fairly presents COMASYSTEM and the related technical and organisational measures and other controls for the period 1 October 2022 to 30 September 2023. The criteria used in making this statement were that the accompanying description:

1. Accounts for COMASYSTEM, and how the general technical and organisational security measures and other controls were designed and implemented, including accounts for:
    - The types of services provided.
    - The processes applied to ensure that the data processing has been performed in accordance with contract, instruction or in agreement with the data controller.
    - The processes that ensure that the staff authorised to process personal data have accepted an obligation of confidentiality or are subject to an appropriate statutory professional secrecy.
    - The processes, which at termination of processing ensure that, at the choice of the controller, all personal data are deleted or returned to the data controller, unless there is a requirement or regulation to store the personal data.
    - The processes, which in the event of breach of personal data security, ensure that the data controller can file a report with the supervisory authority and notify the data subjects.
    - The processes, which ensure appropriate technical and organisational security measures for the processing of personal data considering the risks that processing involve, especially by accidental or illegal destruction, loss, change, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.
    - The controls, which we with reference to the delimitation of COMASYSTEM have assumed 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 supervisory controls relevant to the the processing of personal data.
2. Includes relevant information on changes in COMASYSTEM and the related technical and organisational measures and other controls performed throughout the period 1 October 2022 to 30 September 2023.

3. Does not leave out or misrepresent information relevant to the scope of COMASYSTEM and the relating technical and organisational security measures and other controls considering that this description has been prepared to meet the common needs of a wide range of clients/data controllers and consequently, cannot include all aspects of COMASYTEM that the individual data controller may consider important in their special environment.

COMAsystem ApS confirms that the technical and organisational measures and other controls related to the control objectives stated in the accompanying description were suitable designed for the period 1 October 2022 to 30 September 2023. The criteria used in making this statement were that:

1. The risks threatening the achievement of the control objectives stated in the description 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.

3. The controls were applied consistently as designed, including manual controls were performed by persons with appropriate competencies and rights, in the entire period from 1 October 2022 to 30 September 2023.

COMAsystem ApS confirms that appropriate technical and organisational security measures and other controls have been implemented and maintained for the purpose of complying with the agreements made with the data controllers, generally accepted data processing principles and relevant demands on data processors in accordance with the General Data Protection Regulation and the Data Protection Act.

Copenhagen, 24 October 2023

COMAsystem ApS

Christian Richter-Pedersen
CEO

3. COMASYSTEM APS' DESCRIPTION OF COMASYSTEM AND THE RELATING CONTROLS

INTRODUCTION

The following description of COMASYSTEM has been prepared for the purpose of providing true and fair information as well as information for COMAsystem ApS' clients and external auditors.

Below are a complete description of the system's application, purpose and conditions in relation to the operation of the system. Thereafter, the approach and the ongoing maintenance of the risk assessment for the system are described.

The description also includes an examination of the controls for procedures and documentation implemented by the organisation.

SYSTEM DESCRIPTION

General

COMASYSTEM is a Software as a Service (SaaS) web application, which stores and processes contract data for the users of the system.

Used contract types include:

- Supplier contracts
- Sales contracts
- Staff contracts
- Service contracts

The system enables active utilisation of relevant contract data by means of notifications sent to the responsible users with the customers.

Thus, the system ensures compliance with renewal deadlines, terms of notice, compliance with obligations in relation to staffs and management of service agreements.

The system in its current version has been developed for the purpose of extensive protection of personally identifiable data in accordance with article 25 of the General Data Protection Regulation - "Data protection by design and data protection by default".

Thereby, the system is applied by the customer for contract management, documentation in connection with compliance at processing of personal data and financial optimisation.

Infrastructure and operation

COMASYSTEM is hosted in Denmark, and back-up is also stored in different locations in Denmark.

COMASYSTEM is placed in Global Connect A/S' data centre in Høje-Taastrup, Zealand Denmark. Global Connect A/S solely performs housing tasks and does not act as data processor.

The daily operation of the system, the development and support are conducted solely by COMAsystem ApS and Nordicode ApS, which is data processor.

The use of Nordicode ApS as a data processor has stopped during the period and COMAsystem is now responsible for all development of the application.

Digital Signatur is performed by subsupplier ADDOsign twoday A/S, which acts as data processor for clients, who opt for digital signature.

Back-up is performed by subsupplier FrontSafe ApS, who are data processor.

The system is monitored 24/7 by COMAsystem ApS' own employees. In addition, back-up locations are monitored by FrontSafe ApS. A number of external systems are used for monitoring.

Risk assessment

Premise of the risk assessment
The risk assessment is performed in consideration of the specific information types processed by the system, the amount and the sensitivity of the processed information.

Likewise, the risk of the system is assessed in consideration of the threat(s), which would be relevant for the industries, in which the clients of the system work.

Incidents related to IT or personal data security are included in the ongoing assessment of risks.

The risk assessment has been performed under the assumption of an incident in pursuance of article 32 (2) of the General Data Protection Regulation.

In this connection, it is assumed that the system handles both regular and sensitive personal data.

Assessment and follow-up
The risk assessment has been performed systematically through the following main areas:

- Hardware and system software
- Data transmission
- Applications
- Input data and output data materials
- Organisation - internal
- Subprocessors
- Various incidents of more specific character (future actions)

The risk assessment is used as an active tool and is considered a variable, which must be reassessed currently with regard to ensuring that COMASYSTEM is operated and developed in relation to the risk level required.

For the risk assessment, the system RISMA is used, and the consequence for both the company and the data subject(s) is assessed, in accordance with the General Data Protection Regulation.

All risks are controlled and linked together with processes and/or controls, where these appear of the compliance system applied by COMAsystem ApS.

Risk assessments have been conducted in relation to consequences for both the company and the data subject. The risk assessment is currently reassessed, and processes are in place in connection with Development and new initiatives, which are to ensure that the risk assessment is updated.

It is based on the current threat level and the risk assessment is part of the documentation for the annual ISAE 3000 audit. Based on the audit recommendations, this may form the basis for new projects or procedures, which are to strengthen the security for COMASYSTEM.

SIGNIFICANT CHANGES IN THE PERIOD

There has not been made any significant changes to the application or the infrastructure for the period. The cooperation with Nordicode ApS has stopped and their services are no lunger used to develop the system.

CONTROLS

General

Controls are created and completed in RISMAcontrols. Controls in RISMAcontrols send out e-mails to those responsible for the controls in question, and it is also in RISMAcontrols that the completion of the controls is documented.

The documentation, deviations in connection with control deadline and affiliation to risks and/or processing activities are maintained in RISMAcontrols.

In this way, it is the purpose to create an uniform and continuous overview and history of COMAsystem ApS's control regime.

COMAsystem ApS has an active opinion of the ongoing control regime and currently adapts controls to changed processes or features and adds new or files unnecessary controls.

A.5 Information security policies

An information security policy has been implemented in the company, and it is revised annually.

A.6 Organisation of Information Security

In accordance with the information security policy, the board of directors has the overall responsibility for the organisation of the information security, and COMAsystem ApS' Management has defined an information security strategy. The information security has been unfolded in the entire organisation, and COMAsystem ApS requires the same of external cooperative partners.

A.7 Human Resource Security

It is ensured during the employment of COMAsystem ApS' employees that they can work with confidential matters and are assessed to be capable of handling the operation and the processing of confidential and sensitive data.
There are also procedures which ensure closing of resigned employees.

A.8 Asset Management

The IT Manager has been appointed as the company's system owner and operations manager. The classification of systems and which data are processed have been considered. Processes for protection of mobile IT equipment and server are available. On workstations (mobile equipment) disc encryption has been established. Data-carrying media are destroyed in accordance with approved procedure.

A.9 Access Control

In COMAsystem ApS, procedures for access control on workstations, systems and network have been introduced. Access is granted according to function for the employees in question.

Access to critical operations and back-end systems is protected by firewall and VPN, which is terminated in firewall.

Rotation of passwords according to the minimum requirements of the IT policy has been planned for the VPN users.

Users, who no longer has a function-related need or due to termination of the cooperation, are stripped of rights and/or access to parts of or all systems.

Controls are implemented to monitor that only persons with function-related needs have access to specific systems.

There are no common user accounts, and personal usernames and codes will be provided. Secret codes are managed and stored encrypted.

Access to data-carrying devices and/or critical systems will be according to assessment and in connection with work-related needs.

There are transmission encryption at all log-in features.

A.10 Cryptography

Cryptography is worked with targeted at both transmission of data and in certain cases at storage of data.

For e-mail communication, there are requirements for TLS communication.

For access to web-based services, TLS encryption will be forced at minimum TLS 1.2.

Back-up is transmitted with encryption and are stored with encryption. Front-Safe does not have access to the encryption key for COMAsystem's backup data.

A.11 Physical and Environmental Security

External housing solution is applied for COMAsystem ApS' data centre, where there are 24/7 monitoring and access control.

Only specific COMAsystem ApS' employees with a work-related need have access to the physical material in the data centre. The physical material includes server, switches, firewall, etc. and is owned by COMAsystem ApS.

There is a procedure for secure disposal destruction of data-carrying media.

At COMAsystem ApS, there is an alarm system with alarm calls and processes in place, so that workstations are automatically locked.

A.12 Operations Security

Compliance software is applied for management of processes, control and relating risk assessments. Incidents are recorded according to specific processes, and COMAsystem ApS examines on an annual basis all recorded incidents in connection with process optimisation.

Process and recording for patch management have been set up for both workstations and server.

Operation/capacity monitoring and alarm calls are applied on server.

Centralised software are applied on both work stations and servers to defend against virus and malware.

Back-up has been considered in relation to type and which data to back up. In addition, it has also been considered how often it is necessary to complete back-ups. Back-up is verified according to ongoing control and at application of the system's own verification settings.

Logging has been set up on all operating units and is collected centrally. The access to log data is limited to specific employees.

Change management is recorded in an incident log, and it is solely the IT Manager who is authorised to install and/or change the current software on servers. Employees can with the IT manager's approval receive permission to install software on workstations.

COMAsystem ApS keeps up to date with vulnerabilities in open media and professional network.

A.13 Communications Security

Policies for communications security have been prepared. Solely employees with work-related needs may perform corrections in network equipment.

Mission-critical networks may only be accessed via VPN.

Only relevant and required services are exposed to the open net.

Except forced TLS on all e-mails, internal mail service is applied for comasystem.dk, which is only applied by the application comasystem.dk.

A.14 Development and Maintenance of Systems

There are determined processed for initiation of development and guidelines for security requirements for development, acquisition and maintenance.

Processes are worked with for monitoring and control of subsuppliers.
According to the General Data Protection Regulation, any risk is reassessed currently as well as the requirement for DPIA is reassessed currently.

An uniform Pipeline is applied for development and new system features are documented.

Production and development have been segregated, and production data are not developed.

Processes for updating and upgrading of virtual machines as well as hypervisor and baremetal have been defined.

A.15 Supplier Relationships

Data processing agreements have been entered with subsuppliers and audit opinions have been obtained.

Data processor without assurance reports is audited physically by COMAsystem ApS and without prior notice.

Physical control of data centre's security and surrounding conditions has also been established.

Supervision with primary suppliers is conducted in the following way:

GlobalConnect A/S (not data processor):
Delivery: Data centre housing
- Physical control
- Annual reassessment of audit opinion with special focus on physical security

Nordicode ApS (cooperation has stopped during the period):
Delivery: Development
- Physical control
- Awareness measures
- Logging
- Activity messages

FrontSafe A/S:
Delivery: Back-up
- Function controls (separately during back-up)
- Annual reassessment of audit opinion with focus on exemptions in relation to matters relating to back-up in transmission and during storage

ADDOsign twoDay A/S (formerly known as VISMA):

Delivery: Digital signature

- Annual reassessment of audit opinion with focus on exemptions in relation to matters relating to back-up in transmission and during storage

A.16 Information Security Incident Management

In general, preventive and discovering controls are applied so that personal data breaches may be prevented or managed without undue delays.

There are procedures for managing information security incidents. The management comprises recording, risk assessment, communication and mitigation.

Employees and suppliers are currently made aware of how information security incidents must be handled.

All security incidents are also processed according to the General Data Protection Regulation in connection with recording, orientation and notification.

In most cases, COMAsystem ApS acts as data processor on behalf of the system's clients. Personal data breaches are therefore notified immediately to the relevant data controller(s).

By this, it is specified that COMAsystem ApS's customers are independent data controllers in relation to COMAsystem ApS and have the responsibility for their own risk assessment of incidents and notification to authorities as well as communication to the data subjects.

A.17 Contingency Plans

COMAsystem ApS has procedures in place to ensure start-up of mitigating measures without undue delays in case of system failures or other incidents, which makes COMASYSTEM unavailable for users and COMAsystem ApS' employees or reduces the functionality or security of the system.

In addition, all incidents are also considered incidents under the General Data Protection Regulation and are risk assessed according to this.

In principle, the CEO is responsible in relation to all incidents and arranges recording, communication, risk assessment and mitigation.

CCO takes over this role when the CEO is absent.

All incidents are managed centrally in COMAsystem ApS's compliance software.

A.18 Compliance

Privacy policy has been prepared and is maintained currently via set up control. The policy is available for all COMAsystem ApS' customers and guests on comasystem.dk/privacypolicy.

In relation to awareness training, COMAsystem ApS operates with a very flat organisation and controls are set up, which contributes to repeated discussions and assessments of the conditions of the company in relation to personal data and how employees and suppliers at COMAsystem ApS must handle these.

Data processing agreements with customers are entered when entering agreements/contracts on delivery of COMASYSTEM software and must be signed before access is granted.
The data processing agreement is always available on https://comasystem.dk/dpa.

Data processor record, storage and maintenance hereof take place in the compliance system RISMAgdpr and file-based systems. Record, controls and risk assessment are documented in the system and form the basis for the current documentation of the compiled controls.

Compliance with instructions and notification if these are in contravention of legislation are also kept in RISMAgdpr, and assessments are currently performed via planned controls so that the organisation can be adjusted.

Electronic storage of data processing agreements for suppliers takes place in RISMAgdpr and is compared with the obtained audit opinions.

It is ensured that the subsuppliers meet the requirements from the data controllers through an uniform data processing agreement with COMAsystem ApS's customers and a selection of suppliers, which support the prepared instruction on security level and physical placement. In addition, data processors are risk assessed in relation to the functions, which they perform on behalf of COMAsystem ApS.

Impact assessment (DPIA) is assessed not to be directly necessary to complete due to absence of high risk of the processing and as the processing only to a smaller extent comprises sensitive data. A control has been set up that DPIA for COMASYSTEM is currently reassessed.

Deletion of data is both automated in COMAsystem ApS's backup and in automated processes in the application, which the data controllers have influence on themselves. Client data will be deleted at terminated client relations and are adhered to in the deletion processes. In addition, COMAsystem ApS stores only data, which fall under other legislation, such as the Danish Bookkeeping Act.

The data subjects' rights are described in procedures for COMAsystem ApS. However, the individual client as data controller must extract, correct or delete own data in relation to request, in accordance with article 15-20 and article 7 of the General Data Protection Regulation on consent. In all cases, COMAsystem ApS will assist the data controller according to request, and these requests will be recorded in the incident log for COMAsystem ApS.

Audit and inspection are performed annually and of own motion of COMAsystem ApS. Via external audit of the type ISAE 3000, COMAsystem ApS wishes to illustrate the company's focus on and abilities to work securely and professionally with the customer's data.

Assistance to the data controller is provided to the data controller and the details appear from the data processing agreement.

Controls are set up to handle the protection and documentation of changes, removals or additions of business processes in COMAsystem ApS. The controls will be completed in consideration of the risk assessment, which is based on the consequence for the data subjects.

COMPLEMENTARY CONTROLS WITH THE CONTROLLER

It is requested that the data controllers, which COMAsystem ApS is data processor for, complies with the following:

- To ensure own processes to protect the data subjects' rights for the personal data entered in COMASYSTEM.
- Ensure a sufficient evaluation of the given instruction in the data processing agreement.
- Prepare own risk assessments for obtaining, applying and storing personal data.
- Use the laid down functions in COMASYSTEM for deletion of personal data without purpose or missing legal authority.
- Ensure user administration of own users in COMAsystem so resigned and dismissed employees no longer has access to the system.
- Ensure in the user administration that the granting of rights in COMASYSTEM is cared for.

4. CONTROL OBJECTIVES, CONTROLS, TESTS AND RESULTS OF TESTS

Purpose and scope

BDO has performed their work in accordance with ISAE 3000 on other assurance engagements with certainty than audit or review of historical financial information.

BDO has inspected procedures to obtain evidence of the information in COMAsystem ApS's description of COMASYSTEM, the design and operating effectiveness 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 or operating effectively.

BDO's test of the design and the operating effectiveness 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 COMAsystem ApS, 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 for the period 1 October 2022 to 30 September 2023.

Performed test procedures

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

Type	Description
Inquiries	Interviews of relevant personnel have been performed for all significant control activities. The purpose of the interviews was among other things 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 containing information about the performance of the control, have been read for the purpose of assessing the design and monitoring of the specific controls, and whether the controls are designed so that they can be 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 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 is implemented.
Re-performance	Controls have been re-performed to obtain additional evidence that the controls operate as assumed.

For the services provided by Global Connect A/S as subservice organisation within housing of IT equipment, we have from independent auditor received an ISAE 3402 type 2 assurance report for the period 1 January to 31 December 2022 on the description of controls, their design and functionality in relation to data centre solution.

This subservice organisation's relevant control objectives and related controls are not included in data processor's description of COMASYSTEM and the relating technical and organisational security measures and other controls. Thus, we have only assessed the report and tested the controls with the data processor, who monitors the functionality of the subservice organisation's controls.

For the services provided by FrontSafe A/S as subprocessor within IT operation, we have from independent auditor received an ISAE 3402 type 2 assurance report for the period 1 October 2021 to 30 November 2022 on the cover of the technical and organisational security measures in relation to the operation of Cloud back-up services.

For the services provided by VISMA Consulting A/S as subprocessor within digital signature, we have from independent auditor received an ISAE 3000 assurance report for the period 1 April 2021 to 31 March 2022 on compliance with the Data Protection Regulation of data processor.

Above-mentioned subprocessors' relevant control objectives and related controls are not included in the data processor's description of COMASYSTEM and the relating technical and organisational security measures and other controls. Thus, we have solely assessed the report and tested the controls at the data processor, who ensures appropriate supervision of the subprocessors' compliance with the data processing agreement made between the subprocessor and the data processor and compliance with the General Data Protection Regulation and the Danish Data Protection Act.

Result of test

The result of the tests of technical and organisational security measures and other controls shows whether the tests described has given rise to note exceptions.

An exception exists when:

- Technical or organisational security measures or other controls are to be designed and implemented to fulfil a control objective.
- Technical and organisational measures and other controls related to a control objective are not suitably designed and implemented or did not operate effectively throughout the period.

Risk assessment

Control objectives

- *To ensure that the Data Processor carries out an annual risk assessment in relation to the consequences for the data subjects which forms basis for the technical and organisational measures.*

Control activity	Test performed by BDO	Result of test
Control - Risk assessment ▶ The data processor's information systems and assets are risk assessed in relation to confidentiality, integrity, and availability for the data subject. ▶ At least once a year or at material changes the risk assessment is reassessed. ▶ The company's risk log for information assets is updated in relation to the result of the risk analysis.	We have made inquiries with relevant personnel. We have inspected the data processor's system for risk management and policies for risk management. We observed that the risk assessment has been prepared based on confidentiality, integrity, and availability for the data subject. We observed that the risk assessment is updated at least once a year. We observed that the most recent update of the risk assessment was performed on 6 September 2023. We observed that identified risks are recorded and updated in the data processor's risk log.	No exceptions noted.

A.5: Information Security Policy

Control objectives

- *To provide guidelines for and supporting information security and data protection in accordance with business requirements and relevant laws and regulations. GDPR, article 28(1), article 28(3)(c).*

Control activity	Test performed by BDO	Result of test
Control - Information security policies ▶ Policy for information security policies is established and documented. ▶ Policies for information security will be revised internally at least once a year and at material changes with the data processor.	We have made inquiries with relevant personnel. We have inspected information security policy. We observed that the responsibility and validity area has been defined. We observed that policies include processing of personal data. We observed that the information security policy was updated and approved by Management on 17 September 2023. We also observed that policies and processes were examined together on 7 September 2023.	No exceptions noted.

A.6: Organisation of Information Security

Control objectives

- *To establish a management basis for initiating and managing the implementation and operation of information security and data protection in the organisation. GDPR, article 37(1).*
- *To secure remote workplaces and the use of mobile equipment. GDPR, article 28(3)(c).*

Control activity	Test performed by BDO	Result of test
Policy for organisation of information security ▶ Policy for organisation of information security is established and documented.	We have made inquiries with relevant personnel. We have inspected information security policy. We observed that organisation of information security and responsibility has been defined in the policy.	No exceptions noted.
Roles and responsibilities ▶ All assets and information security processes have been identified, defined, and a responsible party with necessary competences has been appointed. ▶ Responsibility, rights and frame for information security roles have been defined and documented for each process or asset. ▶ The data processor's management ensures that mission-critical duties have been sufficiently segregated. If this is not possible, compensating controls have been implemented.	We have made inquiries with relevant personnel. We have inspected information security policy. We observed that information assets are identified and a responsible party for information security assets has been appointed. We observed that responsibility, framework, and authority have been established and documented in the information security policy. We also observed that implementation of development tasks must be authorised by the company's executive board or board of directors. We have inspected the organisation and roles for segregation of duties for mission-critical systems.	No exceptions noted.
Information security in project management ▶ All projects are risk assessed in relation to information security and personal data. ▶ At material changes in projects, a renewed assessment of the information security must be performed.	We have made inquiries with relevant personnel. We have inspected policies and procedures. We observed that a procedure has been designed for risk assessment in projects. We have inspected documentation for risk assessment. We observed that a risk assessment has been performed in connection with material changes. By inquiry, it was confirmed to us that	No exceptions noted.

A.6: Organisation of Information Security		
Control objectives ▶ *To establish a management basis for initiating and managing the implementation and operation of information security and data protection in the organisation. GDPR, article 37(1).* ▶ *To secure remote workplaces and the use of mobile equipment. GDPR, article 28(3)(c).*		
Control activity	**Test performed by BDO**	**Result of test**
	there have not been material changes during the period, for which reason it has not been possible for us to test the control.	
Policy for mobile equipment ▶ Employees may only install software on workstations after approval by the IT manager. ▶ Workstations are updated automatically via a centrally controlled client. ▶ Workstations are encrypted. ▶ Workstations are installed with active and updated anti-virus software.	We have made inquiries with relevant personnel. We have inspected the Policy for mobile equipment and observed that it states that no software installation is allowed. By inquiry, it was confirmed to us that this can be done with the IT Manager's approval. We have inspected log-in on workstation. We observed that log-in requires user ID and password. By random sampling, we observed that workstations are installed with a client to ensure that updates are installed, and that web shield and anti-virus software have been activated. We observed that the client is administered centrally. We have inspected the system for central management of workstations. We observed that all workstations are installed and updated. By random sampling, we have inspected system configuration of workstations. We observed that workstations are encrypted with BitLocker. We have inspected procedure for control of client. We observed that a procedure has been designed for examination of client. We observed that the control was last updated on 3 September 2023. By random sampling, we have inspected update status for workstation. We observed that the workstation is updated and installed with anti-virus software.	No exceptions noted.

A.6: Organisation of Information Security

Control objectives

- *To establish a management basis for initiating and managing the implementation and operation of information security and data protection in the organisation. GDPR, article 37(1).*
- *To secure remote workplaces and the use of mobile equipment. GDPR, article 28(3)(c).*

Control activity	Test performed by BDO	Result of test
Remote work stations ▶ When working from remote workstations, encrypted VPN is applied. ▶ Documents and devices must be protected against theft, loss, and malicious damage. ▶ Employees are informed about information security when working remotely.	We have made inquiries with relevant personnel. We have inspected VPN system. We observed that encryption of VPN connection has been configured. We observed that the VPN client is authenticated by means of certificate as well as unique user ID and password. We have inspected information security policy. We observed that guidelines for storage and application of IT equipment have been designed. By inquiry, it was confirmed to us that employees are informed of information security when using a remote workstation.	No exceptions noted.

A.7: Human Resource Security

Control objectives

- *To ensure that employees and contracting parties understand their responsibilities and are suitable for the roles they are intended. GDPR, article 28(1), article 28(3), article 37(1).*
- *To ensure that employees and contracting parties are aware of and meet their information security responsibilities. GDPR, article 28(1), article 28(3)(c).*
- *To protect the organisation's interests as part of the change or termination of the employment relationship. GDPR, article 28(3)(b).*

Control activity	Test performed by BDO	Result of test
Policy for human resource security ▶ Policy for human resource security is established and documented. ▶ Policy for human resource security is reviewed annually.	We have inspected information security policy. We observed that policies for human resource security have been established. We observed that policies are revised annually as a part of updating the information security policy. We observed that policies were revised on 7 September 2023, and we also observed that policies and processes were examined together on 7 September 2023.	No exceptions noted.
Before employment ▶ Prior to employment, all candidates are screened and assessed in relation to references, confirmation of education and professional qualifications, verification of identity and in special case, criminal offences. ▶ All employees sign a non-disclosure agreement at employment, of which appear the employee's legal responsibility and sanctions if confidentiality is breached. ▶ Employees are informed of information security and other matters, which are applicable for the position.	We have made inquiries with relevant personnel. We have inspected policies for employment. We observed that there are requirements for obtaining criminal records for all employees at employment. By inquiry, it was confirmed to us that criminal records are obtained for employees at employment. We observed that procedures have been designed for assessment of issuing non-disclosure agreement. By random sampling, we observed that duty of confidentiality is imposed on employees in their employment contract. We observed that the policy includes sanctions at information security policy breaches or confidentiality breaches. We observed that information security has been informed about in connection with employment. We also observed that screening and assessment of candidate have been performed when employing a new employee.	No exceptions noted.

A.7: Human Resource Security

Control objectives

- *To ensure that employees and contracting parties understand their responsibilities and are suitable for the roles they are intended. GDPR, article 28(1), article 28(3), article 37(1).*
- *To ensure that employees and contracting parties are aware of and meet their information security responsibilities. GDPR, article 28(1), article 28(3)(c).*
- *To protect the organisation's interests as part of the change or termination of the employment relationship. GDPR, article 28(3)(b).*

Control activity	Test performed by BDO	Result of test
During employment ▶ The employee is trained in security measures in connection with processing sensitive and confidential data. ▶ Information security policy is available for all employees. ▶ When needed, employees are informed about current threats and changes to information security policies.	We have made inquiries with relevant personnel. By inquiry, it was confirmed to us that information security is trained at employment or when entering cooperative agreements. We have observed that awareness training has taken place e.g., by semi-annual question to the employees. We have inspected shared drive. We have observed that the information security policy is available for all employees. By inquiry, it was confirmed to us that that information security and current threats are informed about, when needed.	No exceptions noted.
Termination of or changes to employment ▶ At employment, all employees are informed about responsibility, requirement and sanctions, which are applicable after termination of the employment.	We have made inquiries with relevant personnel. We have inspected information security policy. We observed that policies for human resource security at resignation have been established. We observed that guidelines have been designed for return of information assets and removal of rights in system. By random sampling, we have inspected documentation for return of information assets, closing of accesses have been performed for the relevant employee, and confidentiality agreement is still applicable.	No exceptions noted.

A.8: Asset Management

Control objectives

- *To ensure adequate protection of information and personal data that is in relation to the importance of the information and personal data for the organisation. GDPR, article 30(3), article 30(4).*
- *To prevent unauthorised disclosure, modification, removal or destruction of information and personal data stored on media. GDPR, article 28(3)(c).*

Control activity	Test performed by BDO	Result of test
Record of assets ▶ Management has prepared, approved, and communicated policies for use and handling of devices and media. ▶ The data processor prepares a written record of the categories of processing activities carried out on behalf of data controllers. ▶ The records are updated currently and controlled during the annual examination of policies and procedures, etc. ▶ The record is stored in writing and electronically. ▶ Upon request, the data processor makes available the record to the supervisory authority. ▶ A system owner who is responsible for the day-to-day operation and maintenance is appointed for all systems. ▶ Data in operation systems is classified and processed as confidential data.	We have made inquiries with relevant personnel. We have inspected information security policy. We observed that policies for use and handling of devices and media have been prepared. We have inspected record of categories and processing activities. We observed that the content thereof complies with the requirements of article 30 (2) of the General Data Protection Regulation. We observed that the record is updated currently. We observed that the record was last updated on 7 September 2023. We observed that record of processing activities is stored electronically. By inquiry, it was confirmed to us that record of categories of processing activities performed on behalf of data controllers is made available for the supervisory authority. We have inspected information security policy. We observed that the IT Manager has been appointed system owner of operation systems. We observed that data in operation systems is classified as sensitive personal data.	No exceptions noted.
Handling of devices and physical media ▶ All devices and media are protected with encryption. ▶ Devices, which are handed over to employees or third parties, are registered at handover and return. ▶ At handover, it is ensured that there are no confidential or sensitive data on the devices.	We have made inquiries with relevant personnel. We have inspected information security policy. We observed that policies for handling physical media and devices have been	No exceptions noted.

A.8: Asset Management

Control objectives

- *To ensure adequate protection of information and personal data that is in relation to the importance of the information and personal data for the organisation. GDPR, article 30(3), article 30(4).*
- *To prevent unauthorised disclosure, modification, removal or destruction of information and personal data stored on media. GDPR, article 28(3)(c).*

Control activity	Test performed by BDO	Result of test
▶ Employees using devices or media outside the organisation are responsible for protecting these against theft, loss or malicious damage.	established. We also observed that guidelines have been established for protection of mobile equipment and devices, which are used outside the organisation. By random sampling, we have inspected system configuration of a workstation. We observed that devices are encrypted. We have inspected policies for using devices outside the organisation. By inquiries, the employees' understanding of the control were confirmed to us.	
Disposal ▶ Discs and media are destroyed, when taken out of operation. ▶ Discs and media are deleted and formatted before reuse.	We have made inquiries with relevant personnel. We have inspected procedures for disposal and deletion of discs. We assess that these have been appropriately designed. By inquiry, we have been informed that there have not been any incidents during the assurance period to use for the test of the effectiveness of the control, for which reason we are not able to comment on this. By inquiry, the employees' understanding of the control were confirmed to us.	No exceptions noted.

A.9: Access Control

Control objectives

- *To restrict access to information and personal data, including information and personal data processing facilities. GDPR, article 28(3)(c).*
- *To ensure access for authorised users and prevent unauthorised access to systems and services. GDPR, article 28(3)(c).*
- *To make users responsible for securing their authentication information. GDPR, article 28(3)(c).*
- *To prevent unauthorised access to systems and applications. GDPR, article 28(3)(c).*

Control activity	Test performed by BDO	Result of test
Policy for access control ▶ Policy for access control to systems and data is established and documented. ▶ Policy for access control is reviewed annually.	We have made inquiries with relevant personnel. We have inspected information security policy. We observed that policies for access control have been established. We observed that policies are revised annually as a part of updating the information security policy. We observed that the policies for access control were revised on 2 July 2023.	No exceptions noted.
Access to network and network services ▶ Access to network and network services requires valid user ID. ▶ When accessing the company network, it is required that VPN is created. ▶ Access is granted to systems and data and is granted users with a work-related need.	We have made inquiries with relevant personnel. We have inspected information security policy. We observed that requirements have been formed for security at access to network and network services. We have inspected system documentation and system configuration for firewall. We observed that access to network requires valid user ID and that access to network is limited. We observed that all connections to operation systems occur via VPN or HTTPS. We have inspected direct access to web services and observed that connection is rejected. We have inspected a list of users with access to VPN. We observed that only employees with a work-related need are granted access.	No exceptions noted.

A.9: Access Control

Control objectives

- *To restrict access to information and personal data, including information and personal data processing facilities. GDPR, article 28(3)(c).*
- *To ensure access for authorised users and prevent unauthorised access to systems and services. GDPR, article 28(3)(c).*
- *To make users responsible for securing their authentication information. GDPR, article 28(3)(c).*
- *To prevent unauthorised access to systems and applications. GDPR, article 28(3)(c).*

Control activity	Test performed by BDO	Result of test
Creation, change and termination of users ▶ A procedure has been designed for change and termination of cooperative relationships. ▶ Creation of users and granting of rights are authorised by the immediate superior. ▶ Allocation of user access is assessed individually and based on the user's functional area. ▶ User is granted a temporary password at creation, which is to be changed at the first log on. ▶ At termination of a cooperative relationship, the user is deactivated in all allocated systems so that access to the company's systems is prevented.	We have made inquiries with relevant personnel. By inquiry, it was confirmed to us that creation of users takes place when entering a contract with an employee. We have inspected procedure for examination of user rights. We observed that examination of rights for critical operation systems and access to personal data takes place. We observed that the control was completed on 2 July 2023. We have drawn a sample on a resigned employee and observed that she has had her accesses removed.	No exceptions noted.
Management of privileged access rights. ▶ Granting of privileged access rights is based on a work-related need. ▶ Privileged access rights are granted to a special user ID.	We have made inquiries with relevant personnel. We have inspected information security policy. We observed that procedures for administration of privileged accesses have been designed. We observed that examination of rights for critical operation systems and access to personal data has been performed. We observed that the control was completed on 2 July 2023, and we have inspected documentation of this. We have inspected documentation showing that privileged access rights are accessed by using a unique user ID.	No exceptions noted.

A.9: Access Control

Control objectives

- *To restrict access to information and personal data, including information and personal data processing facilities. GDPR, article 28(3)(c).*
- *To ensure access for authorised users and prevent unauthorised access to systems and services. GDPR, article 28(3)(c).*
- *To make users responsible for securing their authentication information. GDPR, article 28(3)(c).*
- *To prevent unauthorised access to systems and applications. GDPR, article 28(3)(c).*

Control activity	Test performed by BDO	Result of test
Review of user access rights ▶ Granted access is reviewed twice a year by the system owner.	We have made inquiries with relevant personnel. We have inspected procedure for examination of user rights. We observed that examination of rights for critical operation systems and access to personal data takes place twice a year. We have inspected system for recording of controls. We observed that the revision of granted rights was completed on 2 July 2023, and we have inspected documentation of this.	No exceptions noted.
Management of secret authentication information ▶ Secret authentication information for system and service users is stored with encryption and protected by password. ▶ Only users with special work-related needs have access to passwords.	We have made inquiries with relevant personnel. We have inspected system for storage of secret authentication information. We observed that codes and log-in information are stored, encrypted and protected by password. By inquiry, it was confirmed to us that only employees with work-related needs have access to authentication information.	No exceptions noted.
Limited access to information ▶ Access to system and file system is determined from a work-related need. Granting of access is authorised by the company's management and/or system owner and is examined once a year.	We have made inquiries with relevant personnel. By inquiry, it was confirmed to us that access to information assets and data takes place according to management's order and that granting takes place after an assessment of the work-related need. We observed that only employees with a work-related need are granted access.	No exceptions noted.

A.9: Access Control

Control objectives

- *To restrict access to information and personal data, including information and personal data processing facilities. GDPR, article 28(3)(c).*
- *To ensure access for authorised users and prevent unauthorised access to systems and services. GDPR, article 28(3)(c).*
- *To make users responsible for securing their authentication information. GDPR, article 28(3)(c).*
- *To prevent unauthorised access to systems and applications. GDPR, article 28(3)(c).*

Control activity	Test performed by BDO	Result of test
	By random sampling, we have inspected accesses granted to systems and can confirm that all accesses have been approved. We have inspected procedure for examination of access rights. We observed that examination of rights for critical operation systems and access to personal data takes place. We observed that the control was completed on 2 July 2023, and we have inspected documentation of this.	
Procedures for secure log-on - In case of several failed log-on attempts, user accounts are automatically locked. - When an account is locked and it is not ascribable to the user, this is recorded in an incident log. - Passwords are transmitted with encryption.	We have made inquiries with relevant personnel. By random sampling, we have inspected the system configuration of servers. We observed that there is automatic locking of user accounts at failed log-in attempts. By inquiry, it was confirmed to us that information security incidents are recorded when user accounts are locked, but that there have been no incidents during the assurance period, for which reason we have not been able to test the efficiency of the controls. We observed that log in to system is via HTTPS VPN and that password is encrypted in transmission.	No exceptions noted.
System for administration of passwords - Users are granted a personal user ID. - Users may select and change their own passwords. - Policies and procedures have been designed for passwords to ensure that passwords fulfil the recommen-	We have made inquiries with relevant personnel. We have inspected system configuration for a selected server. We observed that users are created with individual user IDs.	No exceptions noted.

A.9: Access Control

Control objectives

- *To restrict access to information and personal data, including information and personal data processing facilities. GDPR, article 28(3)(c).*
- *To ensure access for authorised users and prevent unauthorised access to systems and services. GDPR, article 28(3)(c).*
- *To make users responsible for securing their authentication information. GDPR, article 28(3)(c).*
- *To prevent unauthorised access to systems and applications. GDPR, article 28(3)(c).*

Control activity	Test performed by BDO	Result of test
dations applicable at any time for protecting passwords with respect to length, complexity, and replacement. All employees have been instructed in selecting and changing passwords. - Passwords are transmitted between client and server with encryption. - Users must change their password at first log-on.	We have inspected user administration system. We observed that users have access to change password. We also observed that it is possible to force users to change password at the next log-in. We have inspected policies and procedures for passwords. We observed that instruction of changing password has been sent to all users. We observed that the instruction includes requirement for selection and change of password. We have inspected documentation for performed control and observed that the last e-mail regarding change of password was sent on 3 September 2023. We have inspected system for authentication. We observed that passwords are transmitted with encryption. By inquiry, it was confirmed to us that users are notified in writing, when starting, that the password must be changed at the first log in.	
Use of privileged system programmes - Use of privileged system programmes on servers requires administrative rights. - Only employees with a work-related need have access to use privileged system programmes.	We have made inquiries with relevant personnel. We have inspected system configuration for a selected server. We observed that use of administrative applications requires membership of privileged group on servers. We have inspected extract of group of rights for a selected server. We observed that access to privileged group is granted to employees with work-related needs.	No exceptions noted.

A.9: Access Control

Control objectives

- *To restrict access to information and personal data, including information and personal data processing facilities. GDPR, article 28(3)(c).*
- *To ensure access for authorised users and prevent unauthorised access to systems and services. GDPR, article 28(3)(c).*
- *To make users responsible for securing their authentication information. GDPR, article 28(3)(c).*
- *To prevent unauthorised access to systems and applications. GDPR, article 28(3)(c).*

Control activity	Test performed by BDO	Result of test
Management of access to source codes for programmes ▶ Access to source code is granted according to work-related needs. ▶ Source code is managed by version in the central storage system. ▶ Access to source code is granted by the IT management. ▶ Access to the storage system is reviewed at least once a year or by creation/closing of projects.	We have made inquiries with relevant personnel. We have inspected system for storage and versioning of source code. We observed that only employees with a work-related need are granted access to the source code and the development system. We observed that source code is version-controlled in central system. We observed that examination of users was performed on 2 July 2023, and we have inspected documentation of this.	No exceptions noted.

A.10: Cryptography

Control objectives

- *To ensure the correct and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information and personal data. GDPR, article 28(3)(c).*

Control activity	Test performed by BDO	Result of test
Policy for use of cryptography ▶ Policy for use of cryptography is established and documented. ▶ Policy for use of cryptography is reviewed at least once a year.	We have made inquiries with relevant personnel. We have inspected information security policy. We observed that policies for application of encryption have been established. We observed that policies are revised annually as a part of updating the information security policy. We observed that policies and processes were examined and assessed together on 7 September 2023.	No exceptions noted.
Protection and encryption of information ▶ Sensitive personal data are protected with encryption, when archived. ▶ All workstations and devices provided are encrypted. ▶ The company's communication connections between the company, customers and cooperative partners are secured with encryption.	We have made inquiries with relevant personnel. We have inspected information security policy. We observed that guidelines have been designed for encryption of data based on requirements for confidentiality and integrity. We observed that policies are revised annually as a part of updating the information security policy. We have inspected file system and back-up system. We observed that data is encrypted during storage. By random sampling, we have inspected a workstation. We observed that it is encrypted. We have inspected test of TLS encryption of data connections to operation systems. We observed that encryption TLS 1.2 and TLS 1.3 for creation of connection has been configured. We have inspected system configuration and that sensitive data are protected with encryption, when archived. We observed	No exceptions noted

A.10: Cryptography		
Control objectives ▶ *To ensure the correct and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information and personal data. GDPR, article 28(3)(c).*		
Control activity	**Test performed by BDO**	**Result of test**
	that encryption is forced when storing passwords. We have inspected logging for applied encryption. We observed that all passwords are encrypted, when archived.	

A.11: Physical and Environmental Security

Control objectives

- *To prevent unauthorised physical access to and damage to and interference with the organization's information and personal data, including information and data processing facilities. GDPR, article 28(3)(c).*
- *To avoid loss, damage, theft or compromise of assets and business interruption in the organisation. GDPR, article 28(3)(c).*

Control activity	Test performed by BDO	Result of test
Policy for physical and environmental security ▶ Policy for physical and environmental security is established and documented. ▶ Policy for physical and environmental security is reviewed at least once a year.	We have made inquiries with relevant personnel. We have inspected information security policy. We observed that policies for physical security have been established. We observed that policies are revised annually as a part of updating the information security policy. We observed that the policies were revised on 7. September 2023. We observed that policies and processes were examined and assessed together on 7 September 2023.	No exceptions noted.
Physical access control - data centre ▶ Access to secured locations is solely granted to employees with work delated needs.	We have made inquiries with relevant personnel. We have inspected access list for persons with access to the data processor's equipment in data centre. Only the CEO and senior developer have been granted access. We observed that the management has revised the granted accesses on 7 September 2023.	No exceptions noted.
Secure disposal, maintenance or reuse of equipment ▶ At disposal, reuse or repair, it is ensured that data is deleted, and that restoration is not possible.	We have made inquiries with relevant personnel. We have inspected controls for disposal and deletion of discs. We have been informed, that there has not been any disposal, reuse of equipment or reparation of equipment. We have therefore not been able to rest the control.	No exceptions noted.

A.11: Physical and Environmental Security

Control objectives

- *To prevent unauthorised physical access to and damage to and interference with the organization's information and personal data, including information and data processing facilities. GDPR, article 28(3)(c).*
- *To avoid loss, damage, theft or compromise of assets and business interruption in the organisation. GDPR, article 28(3)(c).*

Control activity	Test performed by BDO	Result of test
Policy for clean desk and clear screen ▶ PCs must be locked with screen lock when leaving the workplace.	We have made inquiries with relevant personnel. By inquiry of relevant of employees, it was confirmed to us that personal data is not stored in physical form. We observed that automatic screen lock has been implemented when the workstation is left.	No exceptions noted

A.12: Operations Security

Control objectives

- *To ensure proper and safe operation of information and data processing facilities. GDPR, article 25, article. 28(3)(c).*
- *To ensure that information and personal data, including information and data processing facilities are protected against malware. GDPR, article 28(3)(c).*
- *To protect against data loss. GDPR, article 28(3)(c).*
- *To record events and provide evidence. GDPR, article 33(2).*
- *To ensure the integrity of operating systems. GDPR, article 28(3)(c).*
- *To prevent technical vulnerabilities being exploited. GDPR, article 28(3)(c).*
- *To minimise the impact of audit activities on operating systems. GDPR, article 28(1).*

Control activity	Test performed by BDO	Result of test
Policy for operations security ▶ Policy for operations security is established and documented. ▶ Policy for operations security is reviewed annually.	We have made inquiries with relevant personnel. We have inspected information security policy. We observed that policies and guidelines for operations security have been established. We observed that policies for operations security are reviewed annually in connection with revision of the information security policy. We observed that policies and processes were examined and assessed together on 7 September 2023.	No exceptions noted.
Documented operating procedures ▶ Descriptions of procedure or work instructions have been prepared for routine tasks. ▶ Material operational disturbances and irregularities, which impact mission-critical applications, are recorded in an incident log. ▶ Instructions have been prepared for the recovery of mission-critical systems.	We have made inquiries with relevant personnel. We have inspected system for recording of controls. We observed that procedures for returning operational tasks have been designed. We have inspected procedure for significant operational disruptions and irregularities. We have inspected procedure for recording of material operational disturbances and irregularities. We have inspected the incident log. We observed that material operational disturbances are recorded in the incident log.	No exceptions noted

A.12: Operations Security

Control objectives

- *To ensure proper and safe operation of information and data processing facilities. GDPR, article 25, article. 28(3)(c).*
- *To ensure that information and personal data, including information and data processing facilities are protected against malware. GDPR, article 28(3)(c).*
- *To protect against data loss. GDPR, article 28(3)(c).*
- *To record events and provide evidence. GDPR, article 33(2).*
- *To ensure the integrity of operating systems. GDPR, article 28(3)(c).*
- *To prevent technical vulnerabilities being exploited. GDPR, article 28(3)(c).*
- *To minimise the impact of audit activities on operating systems. GDPR, article 28(1).*

Control activity	Test performed by BDO	Result of test
	We have inspected procedure for restoration of operation/contingency plan. We observed that a general plan has been established for restoration of operation after critical failures. We observed that the contingency plan was updated in June 2023.	
Patch management – system software - All material changes are identified, managed, and documented in the Patch Management System. - Testing and deployment are planned as part of the patch management procedure. - All material changes are approved before implementation. - Information security is ensured as part of patch management. - All significant changes undergo risk assessment before implementation. - Emergency procedures and fall-back are planned as part of patch management.	We have made inquiries with relevant personnel. We have inspected system for control documentation. We observed that a procedure has been designed for updating operational systems and databases. We observed that updates are installed and tested in Staging environment before they are installed in operation environment. By random sampling, we have inspected documentation for update. We observed that update of operation systems was completed on 3 September 2023. We observed that a procedure has been designed for updating, including risk assessment and fall-back planning.	No exceptions noted.
Capacity management - Mission-critical systems are monitored in real time for capacity utilisation and lack of resources.	We have made inquiries with relevant personnel. We have inspected system for monitoring of capacity. By random sampling, we observed that monitoring is performed of servers and systems for monitoring of capacity.	No exceptions noted.

A.12: Operations Security

Control objectives

- *To ensure proper and safe operation of information and data processing facilities. GDPR, article 25, article. 28(3)(c).*
- *To ensure that information and personal data, including information and data processing facilities are protected against malware. GDPR, article 28(3)(c).*
- *To protect against data loss. GDPR, article 28(3)(c).*
- *To record events and provide evidence. GDPR, article 33(2).*
- *To ensure the integrity of operating systems. GDPR, article 28(3)(c).*
- *To prevent technical vulnerabilities being exploited. GDPR, article 28(3)(c).*
- *To minimise the impact of audit activities on operating systems. GDPR, article 28(1).*

Control activity	Test performed by BDO	Result of test
	We have inspected documentation for receipt of e-mails with alarms and that they are followed up on.	
Controls against malware ▶ Servers and workstations are protected with anti-virus. ▶ Anti-virus software is updated regularly. ▶ Procedure for handling a malware attack is described and implemented.	We have made inquiries with relevant personnel. By random sampling, we have inspected workstations. We observed that anti-virus software is installed. We also observed that software is updated. By random sampling, we have inspected system configuration for servers. We observed that anti-virus software is installed. We observed that procedure for the users' handling of malware attacks.	No exceptions noted
Information backup ▶ A backup is made of all critical servers and data drives. ▶ Back-up is performed hourly. ▶ Backup is controlled weekly. ▶ Status notification is received when back-up fails. ▶ Once a year, restore test of mission-critical systems is performed.	We have made inquiries with relevant personnel. We have inspected system configuration for back-up. We observed that back-up is performed of mission-critical systems and servers. We observed that back-up is performed every hour. We have inspected system for documentation of controls. We observed that weekly control of correct back-up is performed. We observed that a notification is sent to the operations manager when there are deviations in the back-up.	No exceptions noted.

A.12: Operations Security

Control objectives

- *To ensure proper and safe operation of information and data processing facilities. GDPR, article 25, article. 28(3)(c).*
- *To ensure that information and personal data, including information and data processing facilities are protected against malware. GDPR, article 28(3)(c).*
- *To protect against data loss. GDPR, article 28(3)(c).*
- *To record events and provide evidence. GDPR, article 33(2).*
- *To ensure the integrity of operating systems. GDPR, article 28(3)(c).*
- *To prevent technical vulnerabilities being exploited. GDPR, article 28(3)(c).*
- *To minimise the impact of audit activities on operating systems. GDPR, article 28(1).*

Control activity	Test performed by BDO	Result of test
	We observed that system restoration of server was performed on 3 September 2023.	
Incident logs, protection of log information, administrator and operator log ▶ Mission-critical networks and servers are logged on to, logging is collected and analysed. ▶ Logs are collected and secured in a central database. ▶ Alarms are monitored and handled by head of IT. ▶ Only employees with a work-related need have access to logs. ▶ Systems are time synchronised.	We have made inquiries with relevant personnel. We have inspected system for logging. We observed that logging is performed on critical servers. We observed that logging is consolidated and analysed in a central log system. We have inspected that alarms are monitored and handled by the CEO. We have inspected system for logging. We observed that only employees with a work-related need have access to log system. We have inspected system for logging. We observed that changes in critical system files are logged. We observed that notifications are released when there are changes in system or at creation of users. We have inspected system configuration for SQL server and NTP server. We observed that time synchronisation has been configured for these.	No exceptions noted.

A.12: Operations Security

Control objectives

- *To ensure proper and safe operation of information and data processing facilities. GDPR, article 25, article. 28(3)(c).*
- *To ensure that information and personal data, including information and data processing facilities are protected against malware. GDPR, article 28(3)(c).*
- *To protect against data loss. GDPR, article 28(3)(c).*
- *To record events and provide evidence. GDPR, article 33(2).*
- *To ensure the integrity of operating systems. GDPR, article 28(3)(c).*
- *To prevent technical vulnerabilities being exploited. GDPR, article 28(3)(c).*
- *To minimise the impact of audit activities on operating systems. GDPR, article 28(1).*

Control activity	Test performed by BDO	Result of test
Software installation on operating systems ▶ Software installation on operating systems is subject to change management.	We have made inquiries with relevant personnel. We have inspected system for change management. We observed that procedure has been designed for risk assessment and restoration plan at implementation of changes in operation environment. We have for a sample inspected that risk assessment of change was performed before installation of software.	No exceptions noted.
Technical vulnerability management ▶ Information is currently obtained about vulnerabilities in the applied systems.	We have made inquiries with relevant personnel. We have inspected documentation for collection of information about vulnerabilities and for participating in activities regarding threats and vulnerabilities.	No exceptions noted.
Restrictions applicable to software installation ▶ The IT policy establishes the framework for the use and installation of software. ▶ Installation of software requires prior approval from the company's management.	We have made inquiries with relevant personnel. We have inspected information security policy. We observed that guidelines for application and installation software. By random sampling, we have inspected a workstation to test if installation of software was possible without the management's approval.	We have for one sample noted that that the employee had the possibility to install software without the approval of the management. No further exceptions noted.

A.13: Communications Security

Control objectives

- *To ensure protection of information and personal data in networks and supportive information processing facilities. GDPR, article 28(3)(c).*
- *To maintain information security and data protection when transferring internally in an organisation and to an external entity. GDPR, article 28(3)(c).*

Control activity	Test performed by BDO	Result of test
Policy for communications security ▶ Policy for communications security is established and documented. ▶ Policy for communications security is reviewed annually.	We have made inquiries with relevant personnel. We have inspected information security policy. We observed that policies for communications security have been established. We observed that policies for communications security are reviewed annually in connection with revision of the information security policy. We observed that policy for communications security was last revised and approved by management on 7 September 2023. We observed that policies and processes were examined and assessed together on 7 September 2023.	No exceptions noted.
Network security management ▶ Access to the configuration of network devices is only granted to employees with a work-related need.	We have made inquiries with relevant personnel. We have inspected system configuration for firewall. We observed that access to configuration is granted to employees with on a work-related need.	No exceptions noted.
Security of network services ▶ Access to the company's operation network is protected with encryption.	We have made inquiries with relevant personnel. We have inspected system configuration for firewall. We observed that communication to operation systems is protected with VPN. We observed that the connection is encrypted.	No exceptions noted.

A.13: Communications Security

Control objectives

- *To ensure protection of information and personal data in networks and supportive information processing facilities. GDPR, article 28(3)(c).*
- *To maintain information security and data protection when transferring internally in an organisation and to an external entity. GDPR, article 28(3)(c).*

Control activity	Test performed by BDO	Result of test
Segregation of networks ▶ Services exposed to the internet are protected by firewall.	We have made inquiries with relevant personnel. We have inspected system configuration for firewall. We observed that traffic filtering for access to servers are implemented.	No exceptions noted.
Electronic messaging ▶ The data processor uses e-mail for communication with external parties. The e-mail communication is encrypted during the transmission. ▶ Outbound e-mail communication is scanned when sending sensitive personal data.	We have made inquiries with relevant personnel. We observed that the data processor applies Microsoft Office 365 for e-mail communication. We have inspected system for e-mail. We observed that TLS encryption is forced on all outbound e-mails. We have been informed, that outgoing e-mail communications are not being content scanned when sending sensitive personal data.	We note that outgoing e-mail communications are not being content scanned when sending sensitive personal data. No further exceptions noted.
Confidentiality and secrecy agreements ▶ Written supplier agreements and data processing agreements have been entered or a NDA has been signed, if a supplier has access to or processes personal data, confidential information or sensitive personal data.	We have made inquiries with relevant personnel. By inquiry, we have been informed that no new supplier agreements have been entered during the period, for which reason it has not been possible for us to test the control. We have inspected data processing agreements. We observed that written agreements and data processing agreements have been entered with subprocessor and subservice organisation.	No exceptions noted.

A.14: Acquisition, development, and maintenance

Control objectives

- *To ensure that information security and data protection is an integral part of information systems throughout the life cycle. This also includes the requirements for information systems that provide public network services. GDPR, article 25.*
- *To ensure that information security and data protection are organised and implemented within the information systems development life cycle. GDPR, article 25.*
- *To ensure the protection of data used for testing. GDPR, article 25.*

Control activity	Test performed by BDO	Result of test
Policy for acquisition, development, and maintenance of systems ▶ Policy for acquisition, development and maintenance of systems has been established and documented. ▶ Policy for acquisition, development and maintenance of systems is revised annually.	We have made inquiries with relevant personnel. We have inspected information security policy. We observed that guidelines have been established for security requirements for acquisition, development, and maintenance. We observed that policies for security requirements for acquisition, development, and maintenance are reviewed annually in connection with revision of the information security policy. We observed that policies and processes were examined and assessed together on 7 September 2023.	No exceptions noted.
Analyse and specification of information security requirements. ▶ All projects comprising development or changes of information systems fall within the data processor's procedure for development where information security requirements are mandatory. ▶ Information security requirements are documented in the project documentation. ▶ At new acquisitions, change of outsourcing partner, formation of agreement with new outsourcing partner or the like, a risk assessment is performed. ▶ Systems are designed and implemented so they ensure personal data protection by means of standard settings and through design of processes and functionality.	We have made inquiries with relevant personnel. By random sampling, we have inspected documentation for performed development tasks. We observed that risk assessment of the development task is performed in relation to information security and impact for the data subject. We have observed that requirements for and the result of the risk assessment are documented in the project documentation. We have inspected procedure for development and launch. We observed that risk assessment is updated at material changes in the organisation and IT systems. We observed that changes in subservice organisations and subprocessors imply renewed risk	No exceptions noted.

A.14: Acquisition, development, and maintenance

Control objectives

- *To ensure that information security and data protection is an integral part of information systems throughout the life cycle. This also includes the requirements for information systems that provide public network services. GDPR, article 25.*
- *To ensure that information security and data protection are organised and implemented within the information systems development life cycle. GDPR, article 25.*
- *To ensure the protection of data used for testing. GDPR, article 25.*

Control activity	Test performed by BDO	Result of test
	assessments of threats, which are identified in the threat catalogue and affiliated with subservice organisations and subprocessors. By random sampling, we have inspected risk assessment of changes. We observed that an assessment has been made in relation to whether to carry out a risk assessment. We have inspected procedure for project documentation. We have observed that requirements have been set up for risk assessment and information security requirements, including Privacy by default and Privacy by design.	
Secure development policy ▸ All projects are documented.	We have made inquiries with relevant personnel. We have inspected system for documentation of projects. We observed that there is a procedure for documentation of projects. We have inspected system for Pipeline management. We observed that projects, which are registered in development, are documented.	No exceptions noted.
Principles for development of secure systems ▸ All tasks or changes in systems are assessed for impact on processing of personal data. ▸ Privacy by design and Privacy by default are secured at changes which impact personal data. ▸ The company performs system approval test on components and integrated systems before launch.	We have made inquiries with relevant personnel. We have inspected policies and descriptions of procedures. We observed that at launch of projects, an assessment of the impact of the project in relation to personal data is made.	No exceptions noted.

A.14: Acquisition, development, and maintenance

Control objectives

- *To ensure that information security and data protection is an integral part of information systems throughout the life cycle. This also includes the requirements for information systems that provide public network services. GDPR, article 25.*
- *To ensure that information security and data protection are organised and implemented within the information systems development life cycle. GDPR, article 25.*
- *To ensure the protection of data used for testing. GDPR, article 25.*

Control activity	Test performed by BDO	Result of test
	We observed that design and standard settings are mandatory for assessment at launch of projects. We observed that automated test is performed of source code before installation in operation environment.	
Separation of development, test and operating environments - Rules for transfer of software from development to operation are described in the change management procedure. - Development tests and operating environments for mission-critical systems are separated. - Changes are tested in a separate environment before commissioning. - Data is not stored in development and test environments. - Only the IT Manager has authorisation to installation and/or changes of software. - At deployment of software, notification is sent to CTO.	We have made inquiries with relevant personnel. We have inspected transfer of software from development to operation. We observed that procedure for deployment, test of development projects, bug fixes and transfer of software from development to operation. We have inspected production and test environments. We observed that test and production environments are separated. We observed that test and development are on separate servers. By random sampling, we have inspected system for test of source code. We observed that automated integration test in staging environment has been completed before transfer of software from development to operation. We have inspected documentation for notification at deployment in operation environment. We observed that the IT Manager is notified when new source code for operation environment is sent, before it becomes deployment. We have inspected databases in development and test environments. We observed that data in tables is anonymity.	We noted that segregation of duties related to change and transfer of software from development to operation has not been implemented. This is because developers are granted privileged access to production servers. No further exceptions noted.

A.14: Acquisition, development, and maintenance

Control objectives

- *To ensure that information security and data protection is an integral part of information systems throughout the life cycle. This also includes the requirements for information systems that provide public network services. GDPR, article 25.*
- *To ensure that information security and data protection are organised and implemented within the information systems development life cycle. GDPR, article 25.*
- *To ensure the protection of data used for testing. GDPR, article 25.*

Control activity	Test performed by BDO	Result of test
	We have inspected access systems for access to source code and development tools as well as access to servers.	

A.15: Supplier Relationships

Control objectives

- *To ensure protection of the organisation's assets and personal data that suppliers have access to. GDPR, article 28(2), article 28(3)(d), article 28(4).*
- *To maintain an agreed level of information security, data protection and delivery of services under the supplier agreements. GDPR, article 28(2), article 28(3)(d), article 28(4).*

Control activity	Test performed by BDO	Result of test
Compliance with agreements/handling of security in supplier agreements ▶ It is required that the suppliers' information security level complies with the requirements of the data processor's information security policy. This is secured through contracts, NDA or data processing agreement. ▶ Subprocessor must commit to documenting their compliance with the data processor's information security policy. ▶ Subprocessor must commit to inform the data processor of information security incidents. ▶ The data processor obtains and examines annually ISAE 3000, ISAE 3402 or SOC-2 audit opinion form suppliers of mission-critical services.	We have made inquiries with relevant personnel. We have inspected cooperation agreement with the subservice organisation GlobalConnect A/S. We have inspected data processing agreements and cooperation agreements with GlobalConnect A/S, Nordicode ApS, Visma Consulting A/S and FrontSafe A/S. We observed that the data processor has access to performing audit of processes and controls related to each agreement. We also observed that subprocessors are obligated to inform the data processor about information security incidents. We also observed that subprocessors are obligated to let the data processor perform audit of the subprocessor's processes and controls. We have inspected documentation for supervision of subprocessors. We observed that supervision of subprocessors has been conducted, and that it has been by physical inspection of offices. We have inspected a documentation of this. We have inspected documentation for obtaining and assessing external audit opinions for subprocessors and subservice organisation. We have inspected cooperation agreement with the subservice organisation GlobalConnect as subservice organisation. We observed that an agreement on co-location has been entered. We observed that ISAE 3402 assurance report has been obtained from GlobalConnect A/S as part of the monitoring of the functionality of their controls.	No exceptions noted.

A.15: Supplier Relationships

Control objectives

- *To ensure protection of the organisation's assets and personal data that suppliers have access to. GDPR, article 28(2), article 28(3)(d), article 28(4).*
- *To maintain an agreed level of information security, data protection and delivery of services under the supplier agreements. GDPR, article 28(2), article 28(3)(d), article 28(4).*

Control activity	Test performed by BDO	Result of test
	We have inspected ISAE 3402 assurance report from Global Connect A/S for the period 1 January to 31 December 2022. We observed that it is without any material comments or reservations from the auditor issuing the opinion. We have inspected ISAE 3402 assurance report from FrontSafe A/S for the period 1 October 2021 to 30 November 2022. We observed that it is without any material comments or reservations from the auditor issuing the opinion. We observed that ISAE 3000 assurance report has been obtained from Visma Consulting ApS for the period 1 April 2021 to 31 March 2022. We observed that it is without any material comments or reservations from the auditor issuing the opinion.	
Management of changes in supplier services - At material change of delivery, ownership as well as financial, organisational and other security conditions at the supplier, the service must be reassessed by the data processor.	We have made inquiries with relevant personnel. We have inspected information security policy. We observed that policies for supplier management have been established. We have inspected documentation for performed risk assessments of FrontSafe and VISMA.	No exceptions noted.

A.16: Information Security Incident Management

Control objectives

- *To ensure a uniform and effective method of managing information security breaches and personal data breaches, including communication on security incidents and weaknesses. GDPR, article 33(2).*

Control activity	Test performed by BDO	Result of test
Reporting of information security incidents ▶ All information security incidents, weaknesses and breaches are reported to management. ▶ All information security incidents, weaknesses and breaches are recorded by management in an incident log. ▶ All information security incidents are assessed in relation to confidentiality, integrity, and accessibility.	We have made inquiries with relevant personnel. We have inspected procedure for reporting of information security incidents. We observed that a procedure has been designed for reporting of information security incidents. We have inspected documentation for incidents. We observed that during the period two information security incidents have been reported but are not a breach of the information security. We also observed that the incidents have been mitigated. We observed that an assessment has been made of the reported incidents in relation to whether there has been a personal data breach.	No exceptions noted.
Handling information security incidents ▶ Information security incidents are handled according to an established procedure. ▶ Logging and other evidence are secured in connection with recording of information security incidents.	We have made inquiries with relevant personnel. We have inspected information security policy. We observed that a procedure has been designed for handling information security incidents and breaches, which prescribes that personal data breaches must be reported without undue delay to the data controller. We have inspected an overview of information security incidents. By random sampling, we have inspected documentation for information security incidents. We observed that information security incidents are handled according to procedure.	No exceptions noted.

A.16: Information Security Incident Management

Control objectives

- *To ensure a uniform and effective method of managing information security breaches and personal data breaches, including communication on security incidents and weaknesses. GDPR, article 33(2).*

Control activity	Test performed by BDO	Result of test
Experiences from information security incidents ▶ The company's management examines annually the incident log and initiates improvements of the information security.	We have made inquiries with relevant personnel. We have inspected system for documentation of controls. We observed that a procedure has been designed for examination of all information security incidents and evaluation of these. We have inspected system for documentation of the data processor's controls. We have inspected system for documentation of the company's controls. We observed that examination of the company's incident log has been performed. We observed that the control was performed on 30 July 2023.	No exceptions noted.

A.17: Information Security Aspects of Business Continuity Management

Control objectives

- *To ensure that information security and data protection continuity are rooted in the organisation's management systems for emergency and re-establishment. GDPR, article 28(3)(c).*
- *To ensure accessibility of information- and personal data processing facilities. GDPR, article 28(3)(c).*

Control activity	Test performed by BDO	Result of test
Planning of information security continuity ▶ Based on risk assessment, a plan is established for information security continuity.	We have made inquiries with relevant personnel. We have inspected the contingency plan. We observed that a contingency plan has been design and implemented based on a risk assessment for operation of information assets. We observed that the contingency plan was revised in June 2023.	No exceptions noted.
Implementation of information security continuity ▶ Organisation and management structure during emergency preparedness is specified in procedures for contingency, emergency, and business continuity management. ▶ A general contingency plan has been prepared which describes the overall procedure for initiation of preparedness and organisation of preparedness. ▶ Roles and responsibility in connection with activation of preparedness have been communicated to relevant persons, including information on placement of necessary descriptions and information. ▶ Procedures and work descriptions have been prepared for re-establishment of mission-critical systems.	We have made inquiries with relevant personnel. We have inspected contingency plans. We observed that management structure is specified in the contingency plan. We observed that a general contingency plan has been prepared with procedure for initiation and organisation of preparedness. We also observed that roles and responsibility in connection with preparedness have been established and communicated to relevant employees. We observed that a work description has been prepared for step-by-step re-establishment of operation systems.	No exceptions noted.
Verification, review, and assessment of information security continuity ▶ Contingency plans are audited annually at implementation of new systems or changes in the risk assessment. ▶ Contingency plans are tested according to an established rotation plan. Testing of contingency plans is planned in the annual cycle.	We have made inquiries with relevant personnel. We have inspected the data processor's annual cycle for controls. We observed that procedures have been designed for annual revision of contingency plans. We observed that the contingency plan was revised in June 2023.	No exceptions noted.

A.17: Information Security Aspects of Business Continuity Management

Control objectives

- *To ensure that information security and data protection continuity are rooted in the organisation's management systems for emergency and re-establishment. GDPR, article 28(3)(c).*
- *To ensure accessibility of information- and personal data processing facilities. GDPR, article 28(3)(c).*

Control activity	Test performed by BDO	Result of test
	We have inspected documentation for test of contingency plan and observed that this was performed on 4 and 5 September 2023.	
Availability of information processing facilities - Mission-critical systems are virtualised. - Contingency plans are stored on several physical locations.	We have made inquiries with relevant personnel. We have inspected system configuration for a XEN server. We observed that the data processor's system is virtualised. We have inspected system for storage of documentation. We observed that contingency plans are stored in file system. We also observed that the contingency plan is stored as a physical printout at the office.	No exceptions noted.

A.18: Compliance

Control objectives

- *To prevent violations of statutory, regulatory, or contractual requirements in relation to information security and other security requirements. GDPR, article 25, article 28(2), article 28(3)(a), article 28(3)(e), article 28(3)(g), article 28(3)(h), article 28(3)(f), article 28(10), article 29, article 32(4), article 33(2).*
- *To ensure that information security and data protection is implemented and run in accordance with the organisation's policies and procedures. GDPR, article 28(1).*

Control activity	Test performed by BDO	Result of test
Control - Assistance to the data controller ▶ The data processor has designed and implemented procedures for assistance to the data controller with fulfilling the data subjects' rights. ▶ The data processor has designed and implemented procedures for assistance to the data controller in relation to audit and inspection. ▶ The data controller has designed and implemented procedures for assistance to the data controller in relation to compliance with special requirements of the regulation, including assistance in relation to articles 32-36.	We have made inquiries with relevant personnel. We have inspected data processing agreements and policies. We observed that procedures have been designed for assistance to the data controller in relation to the data subject's rights. We also observed that a standard procedure has been designed for recording of requests from data controllers. By inquiry, we have been informed that the data processor has not received a request from a data controller regarding data subjects' rights during the assurance period, for which reason we were not able to test the efficiency of the controls. We observed that policies and procedures have been designed for the data controller's access to completion of audit and inspection. We have inspected data processing agreements and procedures for assistance to the data controller, in accordance with articles 32-36 of the General Data Protection Regulation, including security of processing, notification and communication at personal data breaches as well as impact assessment. By inquiry, we have been informed that the data processor has not been requested to assist with the stated commitments during the assurance period, for which reason we were not able to test the efficiency of the controls.	No exceptions noted.

A.18: Compliance

Control objectives

- *To prevent violations of statutory, regulatory, or contractual requirements in relation to information security and other security requirements. GDPR, article 25, article 28(2), article 28(3)(a), article 28(3)(e), article 28(3)(g), article 28(3)(h), article 28(3)(f), article 28(10), article 29, article 32(4), article 33(2).*
- *To ensure that information security and data protection is implemented and run in accordance with the organisation's policies and procedures. GDPR, article 28(1).*

Control activity	Test performed by BDO	Result of test
Control - Deletion and return of personal data ▶ There are written procedures containing requirements on storing and deleting personal data in accordance with the agreement with the data controller. ▶ Assessment of whether the procedures are to be updated is made currently and at least once a year.	We have made inquiries with relevant personnel. We have inspected procedure and policies for deletion and return of data to the data controller. We observed that a procedure has been prepared for deletion of data at termination of client relationship. We have inspected log for deletion and performed inspection of databases for recording of personal data. We observed that personal data is deleted according to procedure. We observed that examination of procedures for deletion is planned at least once a year.	No exceptions noted.
Control - Data processing agreements ▶ A procedure has been designed and implemented for obtaining and assessing data processing agreements. ▶ Subprocessors are stated in the data processing agreement with the data controller. ▶ Data processing agreements are signed by data controllers and data processor, and they are archived electronically.	We have made inquiries with relevant personnel. We observed that a standard data processing agreement is used when entering data processing agreements with data controllers and subprocessors. We observed that subprocessors are stated in data processing agreement template with the data controller. By random sampling, we have inspected data processing agreements. We observed that data processing agreements are designed in accordance with article 28 (2) of the General Data Protection Regulation. We observed that the data processing agreements are signed by both data controller and the data processor's management.	We have noted that a former subprocessor still appears for 3 of 6 processing agreements. No further exceptions noted.

A.18: Compliance

Control objectives

- *To prevent violations of statutory, regulatory, or contractual requirements in relation to information security and other security requirements. GDPR, article 25, article 28(2), article 28(3)(a), article 28(3)(e), article 28(3)(g), article 28(3)(h), article 28(3)(f), article 28(10), article 29, article 32(4), article 33(2).*
- *To ensure that information security and data protection is implemented and run in accordance with the organisation's policies and procedures. GDPR, article 28(1).*

Control activity	Test performed by BDO	Result of test
	We also observed that the data processing agreements are stored electronically.	

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
DK-8000 AARHUS C

CVR NO. 20 22 26 80

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Nicolai Tobias Visti Pedersen
Partner, statsautoriseret revisor
På vegne af: BDO
Serienummer: CVR:20222670-RID:1283706411033
IP: 77.243.xxx.xxx
2023-10-24 09:46:41 UTC
NEM ID

Christian Richter-Pedersen
CEO & Partner
På vegne af: COMAsystem
Serienummer: 4328a6a0-06b4-412e-a452-4a418642d03e
IP: 87.116.xxx.xxx
2023-10-24 10:08:10 UTC
MitID

Mikkel Jon Larssen
BDO 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
2023-10-25 09:40:18 UTC
MitID