INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD 1. OCTOBER 2024 TO 30 SEPTEMBER 2025 ON THE DESCRIPTION OF COMASYSTEM AND THE ASSOCIATED TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES AND OTHER CONTROLS, THEIR DESIGN AND OPERATIONAL EFFECTIVENESS RELATING TO THE PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE GENERAL DATA PROTECTION REGULATION AND THE DANISH DATA PROTECTION ACT

COMASYSTEM ApS

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

BDO

CONTENT

1. INDEPENDENT AUDITOR'S OPINION

INDEPENDENT AUDITOR'S ISE 3000 ASSURANCE OPINION FOR THE PERIOD FROM 1 OCTOBER 2024 TO 30 SEPTMBER ON THE DESCRIPTION OF COMASYSTEM AND THE ASSOCIATED TECHNICAL AND ORGANISATIONAL SECURITY MEASURES AND OTHER CONTROLS, THEIR DESIGN AND OPERATIONAL EFFECTIVENESS, AIMED AT THE PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE GENERAL DATA PROTECTION REGULATION AND THE DATA PROTECTION ACT

To: The management of COMAsystem ApS
COMAsystem ApS' Customers (data controllers)

Scope

We have been tasked with providing a declaration of the description prepared by COMAsystem ApS (the data processor) for the entire period from 1. October 2024 to 30. September in section 3 of COMASYSTEM and the associated technical and organisational security measures and other controls, aimed at the processing and protection of personal data in accordance with the Regulation of the European Parliament and of the Council on the protection of natural persons in the in connection with the processing of personal data and on the free movement of such data (the General Data Protection Regulation) and the Act on Supplementary Provisions to the General Data Protection Regulation (the Data Protection Act), and on the design and operational effectiveness of the technical and organisational security measures and other controls linked to the control objectives stated in the description.

Responsibilities of the Data Processor

The Data Processor is responsible for the preparation of the opinion in Section 2 and the accompanying description, including the completeness, accuracy and manner in which the opinion and description are presented. The data processor is also responsible for the provision of the services covered by the description, just as the data processor is responsible for specifying the control objectives as well as designing, implementing and effectively carrying out controls to achieve the stated control objectives.

Auditor independence and quality management

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

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

Auditor's Responsibilities

Our responsibility is to express an opinion on the data processor's description and on the design and operating effectiveness of controls related to the control objectives stated in that Description, based on our procedures.

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

A assurance engagement to provide assurance on the description, design, and operational effectiveness of controls at a processor includes the performance of actions to obtain evidence of the information contained in the processor's description, as well as of the design and operational effectiveness of the controls. The chosen actions depend on the data processor's auditor's assessment, including the assessment of the risks that the description is not true and that the controls are not appropriately designed or do not function effectively. Our actions have included testing the operational effectiveness of such controls, which we deem necessary to provide a high degree of assurance that the control objectives set out in the description were achieved. A assurance assignment with assurance of this type also includes an assessment of the overall presentation of the description, the suitability of the control objectives set out herein and the suitability of the criteria specified and described by the data processor in section 2.

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

Limitations on controls at a data processor

The data processor's description has been prepared to meet the general needs of a wide range of data controllers and therefore does not necessarily include all the aspects of the use of COMASYSTEM that each data controller may consider important according to their particular circumstances. Further, controls at a data processor, due to their nature, may not prevent or detect all personal data breaches. In addition, the projection of any assessment of the operational effectiveness of controls to future periods is subject to the risk that controls at a processor may become insufficient or fail.

Conclusion

Our conclusion is based on the facts set out in this statement. The criteria we have used in formulating the conclusion are the criteria described in the data processor's statement in section 2. This is our opinion:

a. that the description of COMASYSTEM and the associated technical and organisational security measures and other controls, aimed at the 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 throughout the period from 1. October 2024 to 30. September 2025 are fair in all material respects, and

b. that the technical and organisational security measures and other controls associated with the control objectives stated in the description were in all material respects appropriately designed throughout the period from 1. October 2024 to 30. September 2025, and

c. that the tested technical and organisational security measures and other controls, which were those necessary to provide a high degree of assurance that the control objectives set out in the description were achieved in all material respects, have functioned effectively throughout the period from 1. October 2024 to 30. September 2025.

Description of testing controls

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

Intended users and purposes

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

Copenhagen, 10 November 2025

BDO Statsautoriseret Revisionspartnerselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

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

2. COMASYSTEM APS STATEMENT

COMAsystem ApS is responsible for the processing of personal data in connection with COMASYSTEM for our customers who are data controllers in accordance with the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation) and the Act on Supplementary Provisions to the General Data Protection Regulation (the Danish Data Protection Act).

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

COMAsystem ApS uses sub-processors. These sub-processors' relevant control objectives and related technical and organisational measures and other controls are not included in the accompanying description.

COMAsystem ApS confirms that the accompanying description in section 3 provides a true and fair description of COMASYSTEM and the associated technical and organisational security measures and other controls throughout the period from 1. October 2024 to 30. September 2025. The criteria used to give this opinion were that the accompanying description:

1. Describe COMASYSTEM and how the associated technical and organisational security measures and other controls were designed and implemented, including an account of:
    - The types of services provided, including the type of personal data processed.
    - The processes used to ensure that the data processing carried out has taken place in accordance with a contract, instruction or agreement with the data controller.
    - The processes that ensure that the persons authorised to process personal data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality.
    - The processes that ensure that all personal data is deleted or returned to the data controller at the time of the data controller's choice, unless the law or regulation prescribes the storage of the personal data.
    - The processes that in the event of a personal data breach support the data controller's ability to report to the supervisory authority and notify the data subjects.
    - The processes that ensure appropriate technical and organisational security measures for the processing of personal data, taking into account the risks posed by processing, in particular in the event of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
    - The controls that we have assumed with reference to the delimitation of COMASYSTEM would have been designed and implemented by the data controllers, and which, if necessary to achieve the control objectives, are identified in the description.
    - The other aspects of the control environment, the risk assessment process, the information systems and communication, the control activities and the monitoring controls that have been relevant to the processing of personal data.
2. Contains relevant information about changes in COMASYSTEM and the associated technical and organisational security measures and other checks carried out in the period from 1. October 2024 to 30. September 2025.

3. Not omit or distort information relevant to the scope of COMASYSTEM and the associated technical and organisational security measures and other controls, taking into account that this description has been prepared to meet the general needs of a wide range of data controllers and therefore cannot cover every aspect of COMASYSTEM that the individual data controller may consider important according to their particular circumstances.

COMAsystem ApS confirms that the technical and organisational security measures and other controls associated with the control objectives set out in the accompanying description were appropriately designed and functioned effectively throughout the period from 1. October 2024 to 30. September 2025. The criteria used to give this opinion were that:

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

2. The identified controls, if carried out as described, would provide a high degree of assurance that the risks in question did not prevent the achievement of the stated control objectives.

3. The controls were applied consistently as designed, including manual checks being carried out by persons with appropriate competence and authority, throughout the period from 1. October 2024 to 30. September 2025.

COMAsystem ApS confirms that appropriate technical and organisational security measures and other controls have been implemented and maintained in order to fulfil the agreements with the Data Controllers, good data processing practices and relevant requirements for Data Processors in accordance with the General Data Protection Regulation and the Data Protection Act.

Copenhagen, 10 November 2025

COMAsystem ApS

Christian Richter-Pedersen
CEO

3. COMASYSTEM APS DESCRIPTION OF COMASYSTEM

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 utilization 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 optimization.

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 ConnectA/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.

COMAsystem is 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 Unit-IT ApS, who are data processor.

The system is monitored 24/7 by COMAsystem ApS' own employees. In addition, back-up locations are monitored by Unit-IT 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 threats, 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:

- Input data and output data materials
- Users
- Hardware and system software
- Procedures
- General risks
- Subprocessors
- Various incidents of more specific character
    - Future initiatives
    - DPIA
    - Task-specific risk assessments

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, materials from Sikker Digital and others relevant accessible sources are 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 periodically 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 been developed and deployed a new feature for COMASYSTEM that enables complex mapping structures for COMASYSTEM, with an integrated module for asset management in the audit period.

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES AND OTHER CONTROLS

General

Controls which are deemed relevant for the ISAE3000 audit are created and completed in Lexoforms.

ISO 27001 RANGE	CONTROL AREA	ARTICLE
Risk assessment	Risk assessment	Article 28(3)(c)
A.5: Information security policies	Information security policies and information security policy review	Article 28(1)
	Information security policies in accordance with data processing agreements	Article 28(1)
A.7: Personnel safety	Recruitment of employees - Screening	Article 28(1)
	Recruitment of employees - Confidentiality and confidentiality agreement with employees	Article 28(1) and Article 28(3)(b)
	Awareness, education and training regarding information security	Article 28(1)
	Resignation of employees - information about confidentiality and professional secrecy	Article 28(1) and Article 28(3)(b)
	Termination of employees - withdrawal of access rights and assets	Article 28(1)
A.8: Asset Management	List of categories of processing activities	Article 30(2), (3) and (4)
	Repair, service and destruction of IT equipment	Article 28(3)(c)
A.9: Access management	User registration and deregistration and user access rights	Article 28(3)(c)
	Use of secret authentication information	Article 28(3)(c)
	Secure Log-On Procedure	Article 28(3)(c)
	Supporter's access to personal data	Article 28(1)
A.10: Cryptography	Encryption when transmitting personal data	Article 28(3)(c)
A.11: Physical and environmental security	Physical access control	Article 28(3)(c)
A.12: Operational safety	System Software Maintenance	Article 28(3)(c)
	Antivirus program	Article 28(3)(c)
	Data backup and recovery	Article 28(3)(c)
	Logging	Article 28(3)(c)
	Monitoring of systems and environments	Article 28(3)(c)
	Vulnerability scanning and penetration testing	Article 28(3)(c)
A.13: Security of communications	Network security	Article 28(3)(c)
	Firewall	Article 28(3)(c)
	Remote workplaces and remote access to systems and data	Article 28(3)(c)
A.14: Acquisition, development and maintenance	Change management and privacy-by-design	Article 25
	Implementing change in the production environment	Article 25
	Separation of development, test and production environment	Article 25

ISO 27001 RANGE	CONTROL AREA	ARTICLE
	Access to source code	Article 25
	Anonymisation of personal data in development tasks	Article 25
A.15: Supplier relationship	Sub-data processing agreement and instructions	Article 28(2) and (4)
	Approval of sub-processors	Article 28(2)
	Changes in approved sub-processors	Article 28(2)
	The subprocessor's obligations	Article 28(2) and (4)
	Overview of sub-processors	Article 30(2)
	Supervision of sub-processors	Article 28(2) and (4)
A.16: Information Security Breach Management	Notification of personal data breaches	Article 33(2)
	Timely notification of personal data breaches	Article 33(2)
	Identifying personal data breaches	Article 33(2)
	Assistance to data controllers in the event of a personal data breach	Article 33(2)
A.17: Information security aspects of disaster recovery, contingency, and restore management	Planning of information security continuity	Article 28(3)(c)
	Implementation of information security continuity	Article 28(3)(c)
	Verification, review, and assessment of information security continuity	Article 28(3)(c)
	Availability of information processing facilities	Article 28(3)(c)
A.18: Compliance	Procedure for processing personal data	Article 28(3)
	Compliance with instructions for processing personal data	Article 28(3) and Articles 29 and 32(4)
	Agreed security measures	Article 28(3)(c)
	Notification of the data controller in the event of an unlawful instruction	Article 28(3)(h)
	Procedure for fulfilling the rights of data subjects	Article 28(3)(e)
	Technical measures for the fulfilment of data subjects' rights	Article 28(3)(e)
	Deletion of information in accordance with the data controller's requirements	Article 28(3)(g)
	Requirements for the storage and deletion period of data are in accordance with the data controller's requirements	Article 28(3)(g)
	Deletion and return upon termination of customer relationship	Article 28(3)(g)
	Storage of information is in accordance with the data controller's requirements	Article 28(3)(c)
	Location of processing and storage of information	Article 28(3)

Controls are performed and documented by the controlling person and can be completed when relevant comments are added to the evaluation.

In this way, it is the purpose to create a 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 archives unnecessary controls.

A.5 Information security policies
An information security policy has been implemented in the company, and it is revised annually.

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 to systems and data is granted according to function for the employees in question and according to least privilege principles.

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. Unit-IT does not have access to the

encryption key for COMAsystem's backup data.

Customers files are encrypted at rest.

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 and to obtain local admin rights.

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.

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

Unit-IT 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 backup in transmission and during storage

ADDOsign twoDay A/S:
Delivery: Digital signature

- Annual reassessment of audit opinion with focus on exemptions in relation to matters relating to backup 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/ customers 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 OPS board.

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 COMAsystem and file-based systems. Record, controls and risk assessment are documented 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 kept in the OPS board, 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 COMAsystem 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 AT THE DATA CONTROLLERS

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, CONTROL ACTIVITIES, TESTS AND TEST RESULTS

Purpose and scope

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

BDO has carried out actions to obtain evidence of the information in COMAsystem ApS' description of COMASYSTEM as well as of the design and operational effectiveness of the associated technical and organisational security measures and other controls. The actions chosen depend on BDO's assessment, including the assessment of the risks that the description is not true and fair and that the controls are not appropriately designed or do not function effectively.

BDO's testing of the design and operational effectiveness of technical and organisational security measures and other controls has included the control objectives and associated control activities selected by COMAsystem ApS and set out in the subsequent control chart.

In the control form, BDO has described the tests carried out that were deemed necessary in order to obtain a high degree of assurance that the stated control objectives were achieved and that the associated controls were appropriately designed and have functioned effectively throughout the period from 1. October 2024 to 30. September 2025.

Performed test actions

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

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

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 2024 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, which ensures appropriate supervision of the sub-processor's compliance with the data processing agreement made between the sub processor and the data processor and compliance with the General Data Protection Regulation and the Danish Data Protection Act.

For the services provided by Unit-IT A/S as subprocessor within IT operation, we have from independent auditor received an ISAE 3402 and ISAE 3000 type 2 assurance report for the period 1. January 2024 to 31 December 2024 on the cover of the technical and organisational security measures in relation to the operation of Cloud backup services.

For the services provided by Twoday A/S as subprocessor within digital signature, we have from independent auditor received an ISAE 3402 and ISAE 3000 assurance report for the period 1 April 2024 to 31 March 2025 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.

Test result

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

A deviation exists when:

- Technical or organisational security measures or other controls have yet to be designed and implemented in order to meet a control objective.
- Technical or organisational security measures or other controls linked to a control objective have not been appropriately designed and implemented or have not functioned effectively during the period.

Risk assessment

Control objectives

- *To ensure that the data processor performs an annual risk assessment in relation to the consequences for the data subjects, which forms the basis for the technical and organisational security measures.*

Control activity	Tests conducted by BDO	Test result
Risk assessment ▶ A risk assessment is carried out on an ongoing basis and at least once a year based on potential risks to the accessibility, confidentiality and integrity of data in relation to the rights and freedoms of the data subject. ▶ Risks are minimized based on the assessment of their probability, consequence, and derived implementation costs.	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 have been informed by inquiry that the risk assessment is updated on an ongoing basis and at least once a year. Vi observed that the risk assessment has been updated in the declaration period. We observed that identified risks are recorded and updated in the data processor's risk log.	No deviations were found.

A.5: Information security policies

Control objectives

- *To provide guidelines for and support the information security and processing of personal data in accordance with business requirements and relevant laws and regulations – GDPR Article 28(1).*

Control activity	Tests conducted by BDO	Test result
Information security policies and information security policy review ▶ The Data Processor has prepared and implemented an information security policy. ▶ An assessment is made on an ongoing basis – and at least once a year – of whether the IT security policy needs to be updated.	We have carried out enquiry with appropriate personnel at the data processor. 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 29. September 2025.	No deviations detected
Information security policies in accordance with data processing agreements ▶ The data processor's management has ensured that the information security policy is not in conflict with the data processing agreements entered into.	We have carried out enquiry with appropriate personnel at the data processor. We have for a sample inspected data processing agreements to ensure that the requirements in the agreements do not conflict with the information security policy.	No deviations detected

A.7: Personnel safety

Control objectives

- *Ensuring that employees and contractors understand their responsibilities and are suitable for the roles they are intended for – GDPR, Article 28(1).*
- *To ensure that employees and contractors are aware of and live up to their information security responsibilities – GDPR, Article 28(1).*
- *To protect the interests of the organisation as part of the change or termination of the employment relationship – GDPR, Article 28(3)(b).*

Control activity	Tests conducted by BDO	Test result
Recruitment of employees - Screening ▶ The Data Processor carries out screening and background checks on all job candidates in accordance with the Data Processor's procedure and the function that the job candidate must hold.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that formalised procedures are in place to ensure the performance of screening and background checks of the data processor's employees in connection with employment. We have for a sample inspected that the data processor has carried out verification of candidates before employment, and that the checks have included relevant documentation.	No deviations were found.
Recruitment of employees - Confidentiality and confidentiality agreement with employees ▶ Upon employment, employees sign a confidentiality agreement or have otherwise committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality.	We have carried out enquiry with appropriate personnel at the data processor. During the declaration period, we have for a sample inspected that the employees in question have signed a confidentiality agreement in the employment contract.	No deviations were found.
Awareness, education and training regarding information security ▶ An introductory course is held for new employees, including on the processing of data controllers' personal data. ▶ The data processor continuously conducts awareness, training and education of employees in relation to data protection and information security.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that the data processor is conducting an introductory course for new employees, including on the processing of data controllers' personal data. We have inspected that the data processor conducts ongoing awareness, training and education of employees covering general IT security and processing security in relation to personal data.	No deviations were found.

A.7: Personnel safety

Control objectives

- *Ensuring that employees and contractors understand their responsibilities and are suitable for the roles they are intended for – GDPR, Article 28(1).*
- *To ensure that employees and contractors are aware of and live up to their information security responsibilities – GDPR, Article 28(1).*
- *To protect the interests of the organisation as part of the change or termination of the employment relationship – GDPR, Article 28(3)(b).*

Control activity	Tests conducted by BDO	Test result
Resignation of employees - information about confidentiality and professional secrecy ▶ Upon resignation, the employee is informed that the signed confidentiality agreement is still valid.	We have carried out enquiry with appropriate personnel at the data processor. During the declaration period, we have for a sample inspected that the data processor has informed the resigned employees that the duty of confidentiality continues to apply after termination of employment.	No deviations were found.
Termination of employees - withdrawal of access rights and assets ▶ Upon resignation, a process has been implemented by the data processor to ensure that the user's rights become inactive or cease, including that assets are confiscated.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected procedures that ensure that the rights of resigned employees are inactivated or terminated upon resignation, and that assets are confiscated During the declaration period, we have for a sample inspected resigned employees to ensure that rights have been terminated, and that assets have been withdrawn.	No deviations were found.

A.8: Asset Management

Control objectives

- *To identify the organisation's assets and define appropriate responsibilities for their protection – GDPR, Article 30(2), (3) and (4).*
- *To prevent unauthorized disclosure, alteration, removal or destruction of information and personal data stored on media – GDPR, Article 28(3)(c).*

Control activity	Tests conducted by BDO	Test result
List of categories of processing activities ▶ The Data Processor has established a list of categories of processing activities as a Data Processor. The list must include: • the name and contact details of the data controller; • the categories of processing carried out on behalf of the controllers; • the name and contact details of each sub-processor; • indication of any transfer of personal data to a third country. ▶ The record is stored electronically in the data processor's system/file drive. ▶ The data processor will provide the register at the request of the Danish Data Protection Agency.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that the data processor's record of categories of processing activities as a data processor and observed that it contains relevant information, and that the record is stored electronically. On request, we have been informed that the Danish Data Protection Agency has not requested disclosure of the list.	We have established that the Danish Data Protection Agency did not request disclosure of the list at the time of the declaration. We have therefore not been able to test the implementation of this part of the control. No deviations were found.
Repair, service and destruction of IT equipment ▶ The Data Processor has established a procedure for repair, service and destruction of IT equipment that ensures secure handling of IT equipment containing personal data. ▶ The data processor sends IT equipment for repair and service without any personal data. ▶ The data processor disposes of IT equipment by physical destruction of data-bearing media or carries out secure deletion of data on data-bearing media.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that the data processor has formalised procedures for repair, service and destruction of IT equipment. By inquiry, we have been informed that no IT equipment has been sent for repair, service or destruction during the declaration period.	We have established that the data processor has not sent IT equipment for repair, service or destruction. We have therefore not been able to test the implementation of the control. No deviations were found.

A.9: Access management

Control objectives

- *To restrict access to information and personal data, including information and 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 unauthorized access to systems and applications – GDPR, Article 28(3)(c).*

Control activity	Tests conducted by BDO	Test result
User registration and deregistration and review of user access rights ▶ The Data Processor has implemented a procedure for user administration that ensures that user creations and closures follow a controlled process, and that all user creations are authorized and are based on a work-related need. ▶ Privileged (administrative) access rights are granted to systems and devices based on work-related needs. ▶ Users' access is regularly reviewed, including that rights can still be justified by a work-related need.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected information security policy. We observed that policies access management have been established. By inquiry, it was confirmed that user creation takes place after a contract is signed with the employee. We have observed that privileged access rights are granted to systems and devices based on work-related needs. We have inspected procedure for periodic evaluation of user rights. We have observed that evaluation of rights for critical operating systems and access to personal data takes place. We observed that the control was completed on November 29 and December 29, 2024.	No deviations were found.
Use of secret authentication information ▶ The data processor has established rules for password requirements, which must be followed by all employees as well as external consultants.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that users' access to carry out the processing of personal data is done through VPN access and passwords that reflect the risk of the processing activity.	No deviations were found.
Secure Log-On Procedure ▶ The data processor has established logical access control to systems with personal data, including two-factor authentication.	We have carried out enquiry with appropriate personnel at the data processor.	No deviations were found.

A.9: Access management

Control objectives

- *To restrict access to information and personal data, including information and 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 unauthorized access to systems and applications – GDPR, Article 28(3)(c).*

Control activity	Tests conducted by BDO	Test result
	We have inspected that the data processor has established logical access control to systems with personal data, including the use of VPN with private certificate and password.	
Supporter's access to personal data ▶ The Data Processor has established a procedure for supporters' access to personal data, which ensures that supporters' access and handling of personal data in connection with support tasks is based on support tickets and the supporter's work-related needs.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that there are procedures in place to ensure that supporters' access and handling of personal data in connection with support tasks is based on support tickets and the supporter's work-related needs. We have for a sample inspected support cases and observed that these follow the procedure.	No deviations were found.

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 – Article 28(3)(c) of the GDPR.*		
Control activity	**Tests conducted by BDO**	**Test result**
Encryption when transmitting personal data ▶ Encryption is used for the transmission of confidential and sensitive personal data via the internet and e-mail.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected the use of encryption for transmissions of sensitive and confidential personal data via the internet or by e-mail.	No deviations were found.

A.11: Physical and environmental security

Control objectives

- *To prevent unauthorized physical access to, as well as damage and disruption of the organization's information and personal data, including information and data processing facilities – GDPR, Article 28(3)(c).*

Control activity	Tests conducted by BDO	Test result
Physical access control ▶ Physical access controls have been established to prevent the likelihood of unauthorised access to the data processor's offices, facilities and personal data, including ensuring that only authorised persons have access.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that formalised procedures are in place to ensure that only authorised persons can gain physical access to the data processor's premises. We have inspected 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 access on 13. July 2025. We have been informed upon request that the data processor's person information is stored with hosting provider Global Connect. We have inspected hosting provider Global Connect's audit statement and observed that the statement is without reservation and that the statement does not contain matters regarding physical access security that have required further action from the data processor.	No deviations were found.

A.12: Operational safety

Control objectives

- *To ensure the proper and secure operation of information and data processing facilities – GDPR, 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 incidents and provide evidence – GDPR, Article 28(3)(c)*
- *Ensuring the integrity of operational systems – GDPR, Article 28(3)(c).*
- *To prevent technical vulnerabilities from being exploited – GDPR, Article 28(3)(c).*

Control activity	Tests conducted by BDO	Test result
System Software Maintenance ▶ Changes to systems, workstations, databases, and networks follow established procedures that ensure maintenance with relevant updates and patches, including security patches.	We have carried out enquiry with appropriate personnel at the data processor. We observed that a procedure has been designed for updating operational systems and databases. By random sampling, we have inspected documentation for update. We observed that update of operating systems has been performed.	No deviations were found.
Antivirus program ▶ Antivirus is installed for the workstations and systems used for the processing of personal data, which is continuously updated.	We have carried out enquiry with appropriate personnel at the data processor. By random sampling, we have inspected workstations. We observed that antivirus software is installed. We also observed that software is updated.	No deviations were found.
Data backup and recovery ▶ The Data Processor has established a procedure for backup and re-establishment of data and systems that ensures that relevant systems and data are backed up and stored at another physical location, and that systems and data can be re-established.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that formalized procedures are in place to ensure backup and restoration of relevant data and systems, and that backups are stored in another physical location.	No deviations were found.

A.12: Operational safety

Control objectives

- *To ensure the proper and secure operation of information and data processing facilities – GDPR, 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 incidents and provide evidence – GDPR, Article 28(3)(c)*
- *Ensuring the integrity of operational systems – GDPR, Article 28(3)(c).*
- *To prevent technical vulnerabilities from being exploited – GDPR, Article 28(3)(c).*

Control activity	Tests conducted by BDO	Test result
	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. We have inspected that backups have been restored.	

Logging
 	
▸ All successful and unsuccessful access attempts to the data processor's systems and data are logged.
▸ All user changes in the system and databases are logged.
▸ The data processor monitors and logs network traffic.
▸ Security incidents include:
  ○ Changes to log setups, including disabling logging
  ○ Changes to system privileges for users
  ○ Failed log-in attempts to systems, databases and networks
  ○ Brute force
▸ Log information is protected from manipulation and technical errors and is reviewed on an ongoing basis.
	We have carried out enquiry with appropriate personnel at the data processor.
	
	We have inspected that logging of user activities in systems, databases and networks used for the processing and transmission of personal data is configured and enabled.
	
	We have for a sample inspected that periodic review is performed for logs and surveillance.
	
	We have inspected that collected information about user activity in logs is protected from manipulation and deletion.
		No deviations were found.

Monitoring of systems and environments		

A.12: Operational safety

Control objectives

- *To ensure the proper and secure operation of information and data processing facilities – GDPR, 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 incidents and provide evidence – GDPR, Article 28(3)(c)*
- *Ensuring the integrity of operational systems – GDPR, Article 28(3)(c).*
- *To prevent technical vulnerabilities from being exploited – GDPR, Article 28(3)(c).*

Control activity	Tests conducted by BDO	Test result
▶ For the systems and databases used for the processing of personal data, system monitoring with alarms has been established. The monitoring includes: • CPU-load • Ram-usage • Uptime/ downtime	We have carried out enquiry with appropriate personnel at the data processor. 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. We have inspected that the data processor follows up on alarms. We have inspected documentation for receipt of e-mails with alarms and that they are followed up on.	No deviations were found.
Vulnerability scanning and penetration testing ▶ The established technical measures are continuously tested by vulnerability scans and penetration tests. ▶ The data processor reviews the report and deals with identified weaknesses.	We have carried out enquiry with appropriate personnel at the data processor. We have observed that the data processor receives weekly reports from Sophos containing information on threat detections and incidents. We have observed that the data processor has conducted a penetration test. We have inspected the report and found that only minor vulnerabilities were identified, which were not considered necessary to address.	No deviations were found.

A.13: Security of communications

Control objectives

- *To ensure the protection of information and personal data in networks and of supporting information processing facilities – GDPR, Article 28(3)(c).*

Control activity	Tests conducted by BDO	Test result
Network security ▶ Internal networks are segmented to ensure limited access to systems and databases used for the processing of personal data.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected system configuration for firewall. We observed that traffic filtering for access to servers are implemented.	No deviations were found.
Firewall ▶ The data processor has configured the firewall correctly according to best-practice standards. ▶ The data processor only uses services/ports that they need.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that external access to systems and databases used for the processing of personal data is only through the firewall. We have inspected that the firewall is configured according to internal policy for this.	No deviations were found.
Remote workplaces and remote access to systems and data ▶ External access to systems and databases used for the processing of personal data is done by VPN connection.	We have carried out enquiry with appropriate personnel at the data processor. We have observed that remote access to systems and data can only be achieved through VPN. 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.	No deviations were found.

A.14: Acquisition, development and maintenance

Control objectives

- *To ensure that information security and data protection are an integral part of information systems throughout their life cycle. This also includes the requirements for information systems that provide services over public networks – GDPR, Article 25.*
- *To ensure that information security and data protection are organized and implemented within the development lifecycle of information systems – GDPR, Article 25.*
- *To ensure the protection of data used for testing – GDPR, Article 25.*

Control activity	Tests conducted by BDO	Test result
Change management and privacy-by-design ▶ The data processor has established a procedure for development and change tasks that ensures compliance with the privacy-by-design principles, and that all development and change tasks follow a formalized process that ensures testing and requirements for approval before implementation.	We have carried out enquiry with appropriate personnel at the data processor. 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. By random sampling, we observed that automated tests are performed of source code before installation in operation environment.	No deviations were found.
Implementing change in the production environment ▶ The data processor has established a procedure for implementing changes in the production environment that ensures separation of functions in the implementation process.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that no logical separation of functions has been implemented. However, we have identified that internal guidelines have been defined regarding the implementation of changes in the production environment. Furthermore, we have observed that the CEO is notified when new source code is sent to the production environment, prior to deployment.	No deviations were found.
Separation of development, test and production environment ▶ Development and testing are performed in development environments that are separate from production environments.	We have carried out enquiry with appropriate personnel at the data processor.	No deviations were found.

A.14: Acquisition, development and maintenance

Control objectives

- *To ensure that information security and data protection are an integral part of information systems throughout their life cycle. This also includes the requirements for information systems that provide services over public networks – GDPR, Article 25.*
- *To ensure that information security and data protection are organized and implemented within the development lifecycle of information systems – GDPR, Article 25.*
- *To ensure the protection of data used for testing – GDPR, Article 25.*

Control activity	Tests conducted by BDO	Test result
	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.	
Access to source code ▶ Source code is protected from unauthorized modification and deletion.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that only the data processor's developers and CEO have access to source code. We have inspected documentation that the source code is protected against unauthorized modification and deletion.	No deviations were found.
Anonymisation of personal data in development tasks ▶ Anonymized test data is used in the development and test environment.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected development and test databases. We have observed that data anonymized.	No deviations were found.

A.15: Supplier relationship

Control objectives

- *To ensure the protection of the organization's assets and personal data that suppliers have access to – GDPR, Article 28(2) and (4).*
- *To maintain an agreed level of information security, data protection and the provision of services in accordance with the supplier agreements – GDPR, Article 28(2) and (4).*

Control activity	Tests conducted by BDO	Test result
Sub-data processing agreement and instructions ▶ There are written procedures that contain requirements for the data processor when using sub-processors, including requirements for sub-data processing agreements and instructions. ▶ An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that there are formalised procedures for the use of sub-processors, including requirements for sub-data processing agreements and instructions. We have inspected that the procedures have been updated and approved during the declaration period.	No deviations were found.
Approval of sub-processors ▶ The Data Processor only uses sub-processors for the processing of personal data that has been specifically or generally approved by the Data Controller.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that the data processor has a comprehensive and updated overview of the sub-processors used. We have randomly inspected sub-processors from the data processor's overview of sub-processors to ensure that there is documentation that the sub-processors' data processing is stated in data processing agreements entered into with a data controller.	No deviations were found.
Changes in approved sub-processors ▶ In the event of changes in the use of generally approved sub-processors, the data controller is informed in a timely manner in relation to being able to object and/or withdraw personal data from the data processor. In the event of changes in the use of specifically approved sub-processors, this is approved by the data controller.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that there are formalised procedures for notifying the data controller of changes in the use of sub-processors. We have inspected documentation that the data controller has been notified of any change in the use of the sub-processors in accordance with the data processing agreements.	No deviations were found.

A.15: Supplier relationship

Control objectives

- *To ensure the protection of the organization's assets and personal data that suppliers have access to – GDPR, Article 28(2) and (4).*
- *To maintain an agreed level of information security, data protection and the provision of services in accordance with the supplier agreements – GDPR, Article 28(2) and (4).*

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

A.16: Information Security Breach Management

Control objectives

- *To ensure a uniform and effective method for managing information security breaches and personal data breaches, including communication about security incidents and weaknesses – GDPR, Article 33(2).*

Control activity	Tests conducted by BDO	Test result
Notification of personal data breaches ▶ There are written procedures that require the data processor to notify the data controllers in the event of a personal data breach. ▶ An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that there are formalized procedures that contain requirements for notifying the data controllers in the event of a personal data breach. We have inspected that the procedure has been updated and approved during the declaration period. We have inspected that the data processor has an overview of security incidents with an indication of whether the individual incident has resulted in a breach of personal data security. We have inspected documentation for incidents. We observed that during the period information security incidents have been reported but are not a breach of the information security. We also observed that the incidents have been mitigated.	No deviations were found.
Timely notification of personal data breaches ▶ The data processor notifies the data controller of a breach of personal data security without undue delay.	We have carried out enquiry with appropriate personnel at the data processor. We have observed that no incidents have been identified that have led to personal data breaches during the declaration period.	We have found that no incidents have been identified that have led to a breach of personal data security. We have therefore not been able to test the implementation of the control. No deviations were found.
Identifying personal data breaches ▶ The data processor has set up measures to identify breaches of personal data security.	We have carried out enquiry with appropriate personnel at the data processor.	No deviations were found.

A.16: Information Security Breach Management

Control objectives

- *To ensure a uniform and effective method for managing information security breaches and personal data breaches, including communication about security incidents and weaknesses – GDPR, Article 33(2).*

Control activity	Tests conducted by BDO	Test result
	We have inspected that the data processor provides awareness training to employees in relation to the identification of any personal data breaches. We have inspected documentation that network traffic is monitored, as well as that there is follow-up on abnormalities, surveillance alarms, etc.	
Assistance to data controllers in the event of a personal data breach ▶ The Data Processor has established procedures for assistance to the Data Controller in its notification to the Danish Data Protection Agency: • The nature of the personal data breach • Likely consequences of the personal data breach • Measures that have been taken or are proposed to be taken to deal with the personal data breach.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that the procedures available for notifying data controllers in the event of a personal data breach contain detailed procedures for: • Description of the nature of the personal data breach • Description of the likely consequences of the personal data breach • Description of measures taken or proposed to be taken to deal with the personal data breach. We have observed that no incidents have been identified that have led to personal data breaches during the declaration period.	We have found that no incidents have been identified that have led to a breach of personal data security. We have therefore not been able to test the implementation of the control. No deviations were found.

A.17: Information security aspects of disaster recovery, contingency and restore management

Control Objective

- *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 September 2025.	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 September 2025.	No exceptions noted.

A.17: Information security aspects of disaster recovery, contingency and restore management

Control Objective

- *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 18 July 2025.	
Availability of information processing facilities - Mission-critical systems are virtualised, when possible. - Contingency plans are stored on several physical locations.	We have made inquiries with relevant personnel. We have inspected overview of virtualised servers. We observed that the data processor's systems are virtualised, when possible. 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: Conformity

Control objectives

- *To prevent violations of legal, regulatory or contractual requirements in relation to information security and other security requirements – GDPR, Article 28(3), Article 28(3)(a) and (g) and Articles 44 - 49.*

Control activity	Tests conducted by BDO	Test result
Procedure for processing personal data ▶ There are written procedures that require that personal data may only be processed when there is an instruction. ▶ An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that there is a formalised procedure in place to ensure that the processing of personal data only takes place in accordance with instructions. We have inspected that the procedure has been updated and management approved during the declaration period.	No deviations were found.
Compliance with instructions for processing personal data ▶ The data processing agreement contains instructions from the data controller. ▶ The data processor only performs the processing of personal data that is stated in the instructions from the data controller.	We have carried out enquiry with appropriate personnel at the data processor. We have randomly inspected the data processing agreements entered into with a data controller during the declaration period and observed that the agreements contain instructions from the data controller. We have inspected the data processor's record of processing activities and randomly inspected that the processing takes place in accordance with instructions from the data controller.	No deviations were found.
Agreed security measures ▶ There are written procedures that require that agreed safeguards are put in place for the processing of personal data in accordance with the agreement with the data controller. ▶ An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have carried out enquiry with appropriate personnel at the data processor. We have observed that the data processor has implemented the agreed security measures. We have inspected that procedures have been updated and approved during the declaration period.	No deviations were found.

A.18: Conformity

Control objectives

- *To prevent violations of legal, regulatory or contractual requirements in relation to information security and other security requirements – GDPR, Article 28(3), Article 28(3)(a) and (g) and Articles 44 - 49.*

Control activity	Tests conducted by BDO	Test result
Notification of the data controller in the event of an unlawful instruction - The Data Processor shall immediately notify the Data Controller in cases where the Data Controller's instructions are in conflict with data protection legislation.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected the data processor's template for entering into data processing agreements with the data controller and randomly selected data processing agreements with a data controller and observed that the data processor is obliged to notify the data controller in cases where an instruction is deemed to be in conflict with the law. On request, we have been informed that there have been no cases during the declaration period where instructions have been assessed as contrary to legislation.	We have found that there have been no cases where instructions have been assessed as contrary to legislation. We have therefore not been able to test the implementation of the control. No deviations were found.
Procedure for fulfilling the rights of data subjects - There are written procedures that require the data processor to assist the data controller in relation to the rights of the data subjects. - An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that there are formalised procedures in place for the data processor's assistance of the data controller in relation to the rights of the data subjects. We have inspected that the procedures have been updated and approved during the declaration period.	No deviations were found.
Technical measures for the fulfilment of data subjects' rights - The data processor has established procedures which, to the extent agreed, enable timely assistance to the data controller in relation to the disclosure, correction, deletion or restriction of, and information about the processing of, personal data to the data subject.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that the available procedures for assistance to the data controller contain detailed procedures for: • Disclosure of information • Correction of information	We have established that there has been no request for assistance in relation to the rights of the data subjects. We have therefore not been able to test the implementation of the control No deviations were found.

A.18: Conformity		
Control objectives ▶ *To prevent violations of legal, regulatory or contractual requirements in relation to information security and other security requirements – GDPR, Article 28(3), Article 28(3)(a) and (g) and Articles 44 - 49.*		
Control activity	**Tests conducted by BDO**	**Test result**
	• Deletion of information • Restriction of processing of personal data • Information about the processing of personal data for the data subject. We have been informed on request that no request for assistance has been made in relation to the rights of the data subjects during the declaration period.	
Deletion of information in accordance with the data controller's requirements ▶ There are written procedures that require that personal data is stored and deleted in accordance with the agreement with the data controller. ▶ An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that formalised procedures are in place for the storage and deletion of personal data in accordance with the agreement with the data controller. We have inspected that the procedures have been updated and approved during the declaration period.	No deviations were found.
Requirements for the storage and deletion period of data are in accordance with the data controller's requirements ▶ The following specific requirements have been agreed for the data processor's storage periods and deletion routines: • Backup is kept for 180 days.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that the available procedures for storing and deleting personal data contain specific requirements for the data processor's retention periods and deletion routines. We have randomly inspected data processing from the data processor's record of processing activities to ensure that there is documentation that personal data is stored in accordance with the agreed storage periods. We have randomly inspected data processing from the data processor's overview of processing activities to ensure that there is	No deviations were found.

A.18: Conformity		
Control objectives ▶ *To prevent violations of legal, regulatory or contractual requirements in relation to information security and other security requirements – GDPR, Article 28(3), Article 28(3)(a) and (g) and Articles 44 - 49.*		
Control activity	**Tests conducted by BDO**	**Test result**
	documentation that personal data has been deleted in accordance with the agreed deletion routines.	
Deletion and return upon termination of customer relationship ▶ Upon termination of processing of personal data by the Data Controller, data in accordance with the agreement with the Data Controller are: • Returned to the Data Controller, and/or • Deleted where it does not conflict with other legislation.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that formalised procedures are in place for the return and/or deletion of the data controller's data upon cessation of processing of personal data. Upon request, we have been informed that no data processor agreements were terminated during the declaration period. We have been informed that data has been returned to the data controller. We have observed that the data return was carried out with the data controller in accordance with the established procedure.	No deviations were found.
Storage of information is in accordance with the data controller's requirements ▶ There are written procedures that require that personal data is only stored in accordance with the agreement with the data controller. ▶ An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that there are formalised procedures for only storing and processing personal data in accordance with the data processing agreements. We have inspected the deletion logs and conducted an inspection of databases for the registration of personal data. We have observed that personal data has been deleted in accordance with the procedure. We have inspected that the procedures have been updated and approved during the declaration period.	No deviations were found.
Location of processing and storage of information		

A.18: Conformity

Control objectives

- *To prevent violations of legal, regulatory or contractual requirements in relation to information security and other security requirements – GDPR, Article 28(3), Article 28(3)(a) and (g) and Articles 44 - 49.*

Control activity	Tests conducted by BDO	Test result
▶ The data processing by the Data Processor, including storage, may only take place in the locations, countries or territories approved by the Data Controller.	We have carried out enquiry with appropriate personnel at the data processor. We have inspected that the data processor has a comprehensive and updated overview of processing activities with an indication of locations, countries or areas of land for the processing and storage of personal data. We have randomly inspected data processing from the data processor's overview of processing activities to ensure that there is documentation that the data processing, including storage of personal data, is only carried out at the locations stated in the data processing agreements – or has otherwise been approved by the data controller.	No deviations were found.

BDO STATSAUTORISERET REVISIONSPARTNERSELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk

PENNEO

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

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

Nicolai Tobias Visti Pedersen
BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375
Statsautoriseret revisor
På vegne af: BDO Statsautoriseret Revisionspartnerse…
Serienummer: c42f66e9-59bb-478a-9d92-2a2b8602724e
IP: 77.243.xxx.xxx
2025-11-10 11:22:28 UTC

Mikkel Jon Larssen
BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375
Partner, Chef for Risk Assurance
På vegne af: BDO Statsautoriseret Revisionspartnerse…
Serienummer: cd9a38dd-e75c-40f7-80d6-ec5b5d0841d6
IP: 77.243.xxx.xxx
2025-11-10 11:56:46 UTC

Christian Richter-Pedersen
CEO
På vegne af: COMAsystem
Serienummer: 4328a6a0-06b4-412e-a452-4a418642d03e
IP: 87.116.xxx.xxx
2025-11-10 18:36:13 UTC