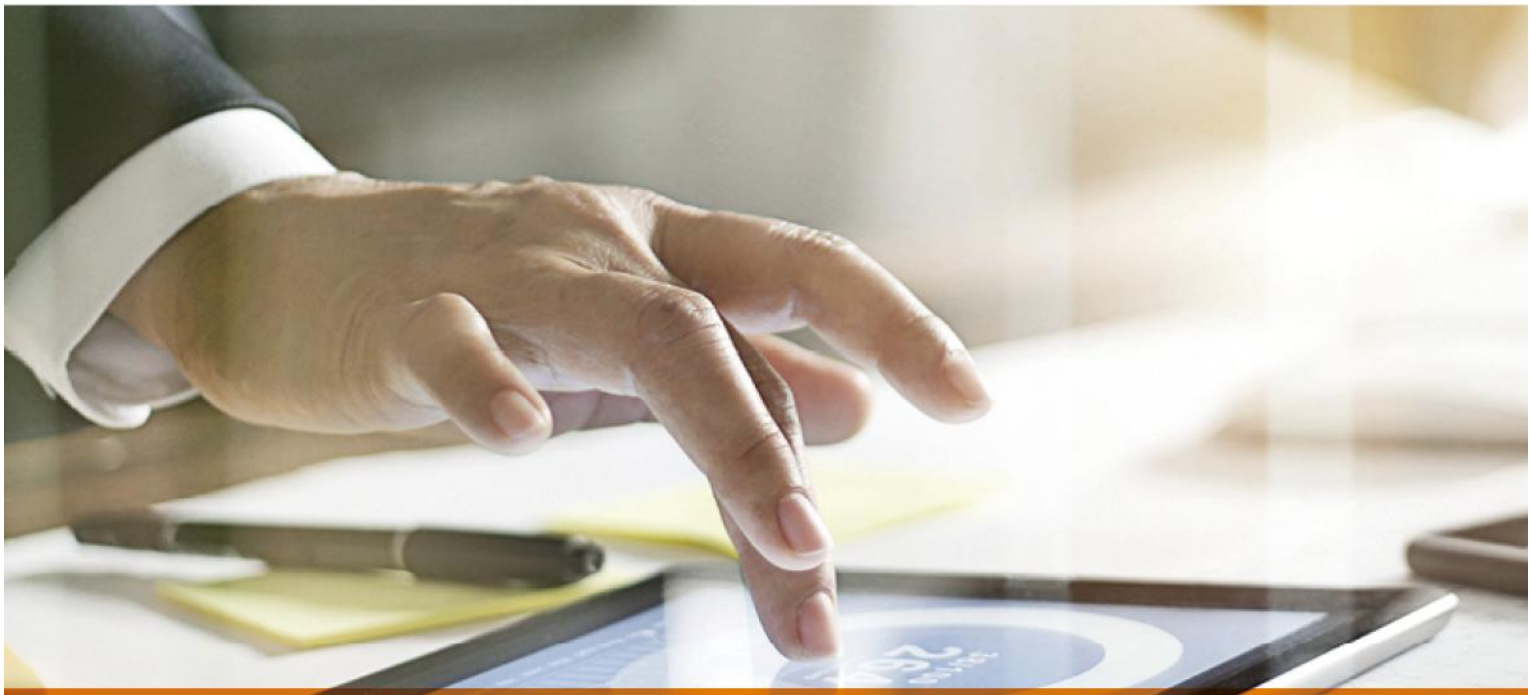
BEIERHOLM
VI SKABER BALANCE



DECEMBER 2020

UNICONTA A/S

ISAE 3402 TYPE 2 ASSURANCE REPORT

CVR 33266928

Independent auditor's report on the control environment related to the operation of Cloud-based ERP system.

In addition, a paragraph has been added to the description about the role as data processor in accordance with the General Data Protection Regulation.

Beierholm
State Authorized Public Accountants
Copenhagen
Knud Højgaards Vej 9
DK-2860 Søborg
Denmark
CVR no. DK 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk

Structure of the Assurance Report

Chapter 1:

Letter of Representation.

Chapter 2:

Description of the control environment for the operation of the Cloud-based ERP system.

Chapter 3:

Independent auditor's assurance report on the description of controls, their design and operating effectiveness.

Chapter 4:

Auditor's description of control objectives, security measures, tests and findings.

CHAPTER 1:

Letter of Representation

Uniconta A/S processes personal data on behalf of Data Controllers according to Data Processor Agreements regarding operation of Cloud-based ERP system.

The accompanying description has been prepared for the use of customers and their auditors, who have used Uniconta A/S' Cloud-based ERP system, and who have sufficient understanding to consider the description along with other information, including information about controls operated by the customers i.e. the Data Controllers themselves, when assessing, whether the demands to the control environment as well as requirements laid down in the General Data Protection Regulation are complied with.

Uniconta A/S hereby confirms that

(A) The accompanying description, Chapter 2 (incl. Appendix 1) gives a true and fair description of Uniconta A/S' control environment in relation to operations of Cloud-based ERP system throughout the period 1 December 2019 - 30 November 2020. The criteria for this assertion are that the following description:

(i) Gives an account of how the controls were designed and implemented, including:

- **The types of services delivered, including the type of personal data processed**
- **The processes in both IT and manual systems that are used to initiate, record, process and, if necessary, correct, erase and limit the processing of personal data**
- **The processes utilized to secure that the performed data processing was conducted according to contract, directions or agreements with the customer i.e. the Data Controller**
- **The processes securing that the persons authorized to process personal data have pledged themselves to secrecy or are subject to relevant statutory confidentiality**
- **The processes securing that - at the Data Controller's discretion - all personal data are erased or returned to the Data Controller, when the data processing is finished, unless personal data must be stored according to law or regulation**
- **The processes supporting the Data Controller's ability to report to the Supervisory Authority as well as inform the Data Subjects in the event of personal data security breaches**
- **The processes ensuring appropriate technical and organizational security measures for processing personal data taking into consideration the risks connected to processing, in particular accidental or illegal actions causing destruction, loss, change, unauthorized forwarding of or access to personal data that is transmitted, stored or in other ways processed**
- **Control procedures, which we assume – with reference to the limitations of Cloud-based ERP system – have been implemented by the Data Controllers and which, if necessary to fulfil the control objectives mentioned in the description, have been identified in the description**
- **Other aspects of our control environment, risk assessment process, information system (including the accompanying work routines) and communication, control activities and monitoring controls relevant for processing of personal data.**

(ii) Includes relevant information about changes in Cloud-based ERP system's processing of personal data performed throughout the period 1 December 2019 - 30 November 2020

(iii) Does not omit or misrepresent information relevant for the scope of the controls described, taking into consideration that the description has been prepared to meet the common needs of a broad range of customers and their auditors, and may not, therefore, include every aspect of

the control system that each individual customer may consider important in their own particular environment.

(B) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period 1 December 2019 - 30 November 2020. The criteria for this assertion are that:

(i) The risks threatening the fulfilment of the control objectives mentioned in the description were identified

(ii) The identified controls would, if used as described, provide reasonable assurance that the risks in question would not prevent the fulfilment of the said control objectives, and

(iii) The controls were applied consistently as designed, including that manual controls were performed by persons with adequate competences and authority throughout the period 1 December 2019 - 30 November 2020.

(C) Appropriate technical and organizational security measures are established in order to honour the agreements with the Data Controllers, compliance with generally accepted data processor standards and relevant demands to Data Processors according to the General Data Processing Regulation.

(D) The accompanying description and the related criteria for fulfilling the control objectives and controls, Chapter 2 (incl. Appendix 1) have been prepared based on compliance with Uniconta A/S' standard agreement as well as related Data Processing Agreement. The criteria for this basis are:

(i) Uniconta – Data Processing Agreement
(ii) Uniconta – Information Security Statement version 1.1
(iii) Uniconta – Information Security Manual Version 1.2 as at 01-11-2020

Ballerup, 9 December 2020

Erik Damgaard, CEO & Founder **Per Pedersen, Director, Sales and Marketing**

Uniconta A/S, Klausdalsbrovej 601, DK-2750 Ballerup, CVR 33266928

CHAPTER 2:

Description of the control environment for the operation of Cloud-based ERP system

Introduction

The purpose of this description is to provide Uniconta A/S' customers and their auditors with information regarding the requirements of ISAE 3402, which is the international auditing standard for assurance reports on controls at service organisations.

The scope of this description is coverage of the technical and organizational security measures implemented in connection with the operation of cloud-based ERP system.

As a supplement to the description below is added an independent paragraph (Compliance with the role as data processor), including a description of essential requirements in connection with the role as data processor combined with general requirements from data processor agreements.

Description of Uniconta A/S

Uniconta is a supplier of ERP software to businesses, organisations and accounting companies. The core activity in Uniconta is the development and operation of the cloud-based ERP system.

The solution is supplied as a service hosted in data centers operated by Uniconta A/S' hosting providers.

Scope of this description

As a supplier of cloud-based ERP system, Uniconta is responsible for establishing and maintaining relevant procedures and controls regarding the development and operation of the Uniconta cloud-based ERP system, ensuring that any security issue is identified and managed according to the requirements laid down in the agreements with the customers.

This description is based on Uniconta's security policies governing the everyday operations of the Uniconta cloud-based ERP system, and the relevant parts of Uniconta's Data Processing Agreement with its customers.

Business strategy / IT security strategy

Uniconta software is designed to be secure, so that neither the customers nor the company is subjected to any unacceptable security risks.

The purpose of Uniconta's IT security strategy is to ensure:

- **The existence of relevant prerequisites for secure operations of the Uniconta cloud-based ERP system**
- **Uniconta software and customer data are sufficiently protected against incidents**
- **Systems and data can be reestablished with predictability and according to familiar working methods**
- **Customer data is accessed by relevant Uniconta personnel, when carrying out necessary tasks**
- **That exclusively authorized persons have access to the operating environment, systems and data**

Uniconta works with IT security at a business-strategic level to ensure a high degree of service and quality. The IT security policy emphasizes the importance of IT security in the company. In relation to its IT security strategy, Uniconta has chosen to take ISO27001+2:2017 as its starting point, and has used the ISO method to implement the relevant security measures within the following areas:

- Information security policies
- Organisation of information security
- Human resources security
- Asset management
- Access control
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance with legal and contractual requirements

In addition, Uniconta's Data Processing Agreement (DPA) binds the company to implement relevant security measures regarding:

- Data processing activities conducted on behalf of the customers
- Data breach monitoring and reporting

The implemented security measures at Uniconta are described in appendix 1.

Uniconta A/S' organization and organization of IT security

Uniconta employs approximately 20 employees and has a flat organizational structure. The CEO manages the company together with the senior management group.

In order to ensure the correct level of focus on information security, Uniconta has appointed a specific Information Security Board acting on behalf of the management and taking the responsibility of security issues. In 2020, the Committee consisted of:

- Per Pedersen, Executive Vice President
- Jørn Rejndrup, Executive Vice President

Risk management at Uniconta A/S

The purpose of the information security policy is to define a framework for the protection of valuable information and, in particular, to ensure that critical and sensitive information and information systems maintain their confidentiality, integrity and accessibility.

Therefore, Uniconta's management has chosen a risk-based information security management system, ensuring that all notable threats are mitigated in an appropriate manner. This way, predictable security problems can be prevented and potential damage limited, ensuring effective restoration of information in case of an incident.

The risk management policy is established to cover or limit the risks created by everyday activities to a level enabling the company to maintain normal operations. Uniconta carries out risk management and internal checks in relevant areas and levels: the risk and impact assessment process is executed annually, in order to keep the management aware of the risk profile of Uniconta. Risk assessments are also conducted, if significant changes take place in the company.

Uniconta has carried out a risk analysis and drawn up the Uniconta Information Security Management System based on the results of the risk assessment. Furthermore, an incident response policy with a corresponding disaster recovery plan has been created utilizing the outcome of the risk management process.

Uniconta also works with the known international standards for IT security. The ISO27001+2:2017 is the primary reference framework for IT security used at Uniconta. The work process regarding IT security is a continual and dynamic process, ensuring that Uniconta at all times complies with its customers' needs, and with legal and contractual requirements.

IT security execution

The management of Uniconta has the day-to-day responsibility for IT security, ensuring that the overall requirements and framework for IT security are maintained. To ensure that information security is appropriately addressed at Uniconta, the management has appointed an Information Security Board to handle security related work in Uniconta.

The structure of the Uniconta ISMS is described in the central IT security policy prepared by the management. The aim of the Uniconta ISMS is to provide the company with a common set of rules and guidelines regarding information security, ensuring a stable and secure operating environment. Uniconta makes regular improvements to policies, procedures and operations to ensure that both our customers' requirements and relevant legislation are complied with.

Uniconta's IT security focus is on everyday development and operations, and the ability to ensure that a well-functioning Uniconta offers services to the customers at an acceptable level. The ISMS applies to all employees without exception, both permanent and temporary staff, and, where relevant, to outsourced workforce working for Uniconta.

When outsourcing parts of Uniconta's development or operations, the service provider must cooperate with Uniconta to ensure the appropriate security level as well as ensuring operations being executed in accordance with the Uniconta ISMS. Uniconta protects its information and solely allows use of and access to information in accordance with the company's guidelines and current legislation.

HR, employees and training

Uniconta acknowledges the fact, that its employees play an important role in the Information security of the company. Uniconta has therefore implemented measures to ensure processes concerning information security prior, during and after employment. The Executive Vice-President and direct line managers have specified responsibilities to perform the relevant tasks set out in the specific guidelines.

All individuals employed by Uniconta are subject to screening prior to employment. The screening follows the defined process.

Employees are furthermore contractually informed and obligated to follow the rules and guidelines set out by the management of Uniconta regarding information security.

During the employment at Uniconta, individual employees are obligated to participate in the information security awareness-training program covering both GDPR and general information security topics.

And in the case of termination of employment, Uniconta has a defined procedure to ensure that the relevant it-equipment is returned, and user access rights are closed or in other ways handled.

Asset management

Uniconta has limited ownership of physical assets. Trusted suppliers primarily deliver operating servers and IT-infrastructure. Uniconta has an interest in ensuring that all assets are securely operated. Uniconta has therefore assigned ownership of each assets to specific employees within Uniconta.

Ownership of an asset means that the specified employee has the responsibility of ensuring that the asset is implemented and operated with respect to the overall objectives for the information security of Uniconta.

Ownership of assets can be delegated from the management to relevant employees.

Ownership of hardware and software assets is documented, reviewed and adjusted as part of the annual risk assessment process.

Access control

Physical and logical access control is of priority in Uniconta. There is a clear motivation to control access to Uniconta's assets and limit it to the people who have a clear need-to-know and tasks related to the access given.

Uniconta's overall guidelines to controlling the access to assets are documented in the access control policy.

Access control is focused around 1) access to the Uniconta IT-infrastructure and 2) access within the Uniconta-application:

1) IT-infrastructure: Uniconta is dependent on suppliers for the IT-infrastructure and sets demands for the suppliers in terms and access management and user rights.

2) Within Uniconta-Application: For the Uniconta-application, a logical layered access control scheme is implemented, which ensures that the relevant user types (both internal and external) have the appropriate access within the Uniconta system and underlying data.

Access control related to Uniconta's own network is defined in the Network Access Control Policy.

Physical and environmental security

Uniconta's offices are in a shared office space at the premises of the Danish insurance company, Tryg, in Copenhagen, Denmark. This means that there are high standards for the physical security and access to the offices. All employees have personal id-cards, which must be used for access. All visitors are registered in the reception area and there are physical barriers preventing unauthorized access to the building and office areas.

The IT infrastructure (servers) from where the Uniconta application is being operated is physically located in a data centre in Denmark. Uniconta has entered into an agreement with the company, Hostingkompagniet who are responsible for the physical security of the servers.

Employees are instructed to follow guidelines related to the daily work routines.

Operation Security

In order to ensure an appropriate level of operational security, Uniconta has applied a variety of controls addressing security issues, covering:

- Firewall
- Backup
- Patch management procedures
- Malware protection
- Monitoring
- Log management/SIEM
- Technical vulnerability management
- Separation of development, test and production environments

The overview below will cover the parts of the policies considered relevant for external stakeholders.

Separation of development, testing, and operation environments
Uniconta has separate environments for development, test and production. The purpose of separate environments for development, test and production respectively is to ensure a continuous development of the cloud-based ERP system, while making sure that only changes which have been appropriately tested are launched into the production environment.

Backup and recovery
The backup policy ensures appropriate protection against loss of data and ensures the ability to restore production data that has been lost or corrupted in the client's system.
Backup copies of information, software and system images are taken and tested regularly in accordance with Uniconta's backup setup rules.

Logging and monitoring
Uniconta logs system events and selected applications locally using a central logging solution. The logging facilities and log information are protected against tampering and unauthorized access.

Management of technical vulnerabilities
Uniconta conducts continuous testing in order to identify technical vulnerabilities of information systems being used in Uniconta. In case of severe vulnerabilities being found, the exposure to such vulnerabilities is evaluated and appropriate measures are taken to reduce the risks to everyday operations.

Communications security

Uniconta uses primarily two networks, one for the office space and one for servers.

Uniconta's use of office network is limited to workstations and shared office resources, such as printers. The employees' use of the network is regulated by rules laid down in the IT-usage guidelines. Access to the network requires the assignment of connection right to the network.

The server network is operated by Hostingkompagniet and is strictly used for connection of the Uniconta servers only. This means that several security measures are implemented on the network.

Networks are in this way segregated by default: One network for employees and workstations and another network for the UC-application.

System acquisition, development and maintenance

The development of the Uniconta cloud-based ERP system is one of the primary activities of Uniconta. The quality and stability of the ERP system has a direct influence on the overall company.

Therefore, there is a strong focus on securing that the development of the ERP system meets the requirements of Uniconta's customers and partners.

Uniconta has established separate environments for the development, test and production of the cloud-based ERP system.

The overall goal is to ensure that updates and new developments meet high standards by monitoring development, testing and approving processes before release and at the same time maintain a flexible approach, which enables Uniconta to constantly develop the ERP system.

Uniconta has established guidelines and processes for the development and release of updates.

These guidelines include:

- Defined responsibilities
- Guidelines for development
- Categorization of bugs and developments task
- Development process
- Testing process
- Release process

Supplier relationships

Uniconta works with suppliers in operating and developing the Uniconta cloud-based ERP system. For key suppliers, who have access to customer instances, it is mandatory to have GDPR-compliant sub-processing agreements in place with Uniconta, compelling the suppliers to follow the same regulations as Uniconta. Relevant suppliers must also be compliant with Uniconta's information security policies. Uniconta is dependent on a few key suppliers in its daily operation and development of the Uniconta cloud-based ERP system.

See below for a short description of Uniconta' main type of suppliers regarding the development and production of the Uniconta software application:

1) Outsourcing partners for development resources – Uniconta recruits and facilitates IT development resources through key suppliers
2) Hosting provider – Responsible for the operation and support related to the IT infrastructure of Uniconta (servers).
3) TRYG – responsible for operating the physical office space and network access in the office.

All supplier relationships are governed through formal agreements.
To ensure that information security is evaluated and prioritized before entering into agreements with new suppliers, Uniconta has defined specific policies for selection of suppliers.
Agreements with key suppliers are reviewed annually.

Managing IT security incidents

Uniconta incident management policies are devised to ensure quick detection, reaction and response to security incidents, and to outline the processes following a security incident.

All employees at Uniconta are familiar with the procedures for reporting different types of incidents and weaknesses, which can influence operational security. Security incidents and weaknesses must be reported as quickly as possible to the management group.

The management group is responsible for defining and coordinating a structured management process that ensures an appropriate reaction to security incidents. All Uniconta's employees, partners, contractors and suppliers have a responsibility to report security incidents and data breaches as quickly as possible to Uniconta's Executive Vice-President. This obligation also extends to any external organisation contracted to support or access the Uniconta Information Systems.

Uniconta is responsible for the security and integrity of all the data, it keeps. Uniconta protects data using all means necessary: incidents affecting data security are prevented and/or minimized in the best way possible. In case of an identified data breach, Uniconta follows a specific data breach handling process.

All critical incidents are handled according to Uniconta's incident handling process, and an incident report is produced and shared with the customer affected by the incident. Reporting critical incidents causes relevant Uniconta employees and managers to be alerted to ensure efficient incident handling.

Review of the event will be undertaken by the Executive Vice President together with relevant employees and managers to establish the cause of the incident, the efficiency of the response and to identify areas that require improvements. Lastly, recommended changes to systems, policies and procedures are documented and implemented as soon as possible.

Information security aspects of business continuity management

Uniconta has a business continuity plan, which defines the actions needed to be taken in the case of security incidents that are affecting the Uniconta application.

Measures have been implemented to ensure that the production environment is protected and that relevant redundancies are in place and that service can be restored in case of hardware and/or software failures.

Compliance with the role as Data Processor

It is the responsibility of Uniconta's management to ensure that all relevant legal and contractual requirements are identified and complied with correctly. Relevant requirements might be, e.g:

- The EU General Data Protection Regulation
- The Danish Data Protection Act
- Data Processor Agreements
- Uniconta A/S standard contract or other relevant sources

The existence of all necessary agreements, a comprehensive ISMS (management system for managing information security) as well as other relevant documents, ensure compliance with all relevant legal and contractual requirements.

Uniconta is obliged to involve legal experts as needed to ensure compliance with law and regulations.

Furthermore, Uniconta's senior management reviews all Uniconta's security policies on a regular basis, including involving any relevant stakeholders. Uniconta's ISMS is regularly audited by an independent, external party, and on request the audit report is shared with all Uniconta's customers.

The EU General Data Protection Regulation (GDPR)

The Uniconta cloud-based ERP system enables our customers to collect, process and report on data they collect from respondents or other data inputs. Uniconta does not own the data our customers collect but develops and operates the software for our customers to utilise.

According to the EU General Data Protection Regulation and Danish additional regulation (The Danish Data Protection Act), Uniconta is the Data Processor, and the customer is the Data Controller.

Uniconta cooperates with legal experts to ensure that all legal requirements are identified and accommodated. Uniconta has also ensured relevant contracts with all key stakeholders (including customers, business partners, key suppliers etc.) to ensure compliance with law and regulations. In addition, Uniconta works together with the customers to ensure that the customers are aware of and comply with the relevant GDPR rules.

According to GDPR, compliance with the ISO27001+2:2017 standard ensures an appropriate security level. Besides compliance with the relevant ISO requirements, Uniconta ensures data privacy and data security on a contractual level.

Privacy and protection of personal data

As mentioned above, Uniconta is the customers' Data Processor, given that the customers are offered an IT service to which they can to transfer and process data, and utilize it for further processing within their respective administrative assignments. Uniconta is not responsible for any data uploaded by the customers to their Uniconta IT service. Based on the categories and confidentiality of the data entrusted to Uniconta by the customers, Uniconta must put all necessary security measures required into practice to ensure an appropriate level of security.

Below is described Uniconta's procedures of how Uniconta operates as Data Processor according to directions from the Data Controllers.

Data Protection Agreements

Uniconta has Data Processor Agreements (DPA) in place with all of our customers. These contracts outline Uniconta's role and responsibilities as Data Processor, and the customer's role and responsibilities as Data Controller.

According to our standard DPA, Uniconta keeps a record of processing activities carried out on behalf of our customers. The records include:

- **The name and contact information of the supplier, the sub-processors, and the customer.**
- **The categories of processing carried out by the supplier or any sub-processors on behalf of the customer.**
- **Transfer of personal data, if any, outside of EEA, including the name of any sub-processor and the concerned country or countries outside of EEA.**
- **Where possible, a general description of the technical and organisational security measures undertaken by the supplier to safeguard the personal data.**

Access to the data in customer instances

In general, Uniconta does not access any customer instances unless specifically appointed by the customer.

In short, Uniconta does not access the data collected by its customers, unless specifically asked by the customer. Only specific employees at Uniconta are allowed to access customers' data upon request.

Important changes in relation to IT security

During the period covered by the report, there have been no significant changes in relation to IT security.

Customers' responsibilities (complementary controls at the customer)

The above description is based on the Uniconta ISMS and other standard contractual clauses. This means that no account has been made for the agreements of individual customers.

Uniconta expects the customer to handle the access control to the customer's own instance. Uniconta grants the access to an appointed person working for the customer during onboarding, and afterwards it is the customer's responsibility to ensure that the access rights to their instance are appropriately controlled. The customer must have relevant access control restrictions in place in order to ensure the security of their Uniconta instance.

The responsibility for the daily use of Uniconta's platforms and customizations herein lies with the customer. Uniconta is not responsible for the customer's use of the software; it is the customer's own responsibility to ensure that the necessary internal security controls are in place, when using the Uniconta cloud-based ERP system. In general, Uniconta recommends risk-based evaluations to take place

when planning any changes to a Uniconta instance: as the customer has the option to modify their instance, the potential risks created by the modifications should always be assessed and limited.

Furthermore, Uniconta does not take the responsibility regarding the data a customer collects and processes using their Uniconta instance. As described above, Uniconta does not access any customer instances, unless specifically asked by the customer, thus Uniconta does not know, what kind of data the customer is collecting.

APPENDIX 1:

Uniconta A/S applies the following control objectives and security measures from ISO27001+2

0. Risk Assessment and management
- 0.1. Assessment of security risks
- 0.2. Risk management

5. Information Security Policies
- 5.1. Management directions for information security

6. Organisation of Information Security
- 6.1. Internal organisation

7. Human Resource Security
- 7.1. Prior to employment
- 7.2. During employment
- 7.3. Termination or change of employment

8. Asset Management
- 8.1. Responsibility for assets
- 8.3. Media handling

9. Access Control
- 9.1. Business requirements of access control
- 9.2. User access management
- 9.3. Users' responsibility

11. Physical and environmental security
** Limited responsibility**
- 11.1. Secure areas
- 11.2. Equipment

12. Operations Security
** Limited responsibility**
- 12.1. Operational procedures and responsibilities
- 12.2. Protection from malware
- 12.3. Backup
- 12.4. Logging and monitoring
- 12.5. Control of operational software
- 12.6. Technical vulnerability management

13.Communications Security
** Limited responsibility**
- 13.1. Network security management

14. System acquisition, development and maintenance
- 14.1. Security requirements of information systems
- 14.2. Security in development and support processes
- 14.3. Test data

15. Supplier Relationships
- 15.1. Information security in supplier relationships
- 15.2. Supplier service delivery management

16. Information Security Incident Management
- 16.1. Management of information security incidents and improvements

17. Information Security Aspects of Business Continuity Management
- 17.1. Information security continuity
- 17.2. Redundancies

18. Compliance
- 18.1 Compliance with legal and contractual requirements

** Limited responsibility **

Responsibility for compliance with the control objective is divided between Uniconta A/S and the subcontractors.

See description of controls in relation to covering the control risk, including how Uniconta A/S continually supervises operations security and data security.

CHAPTER 3:

Independent auditor's assurance report on the description of controls, their design and operating effectiveness

For the customers of Uniconta A/S' Cloud-based ERP system and their auditors

Scope

We have been engaged to report on Uniconta A/S' description in Chapter 2 (incl. Appendix 1), which is a description of the control environment in connection with the operations of Cloud-based ERP system, see Data Processor Agreements with customers, throughout the period 1 December 2019 - 30 November 2020, as well as on the design and function of controls regarding the control objectives stated in the description.

We express our opinion with reasonable assurance.

The report is based on a partial approach, which means this report does not includes the IT security controls and control objectives related to use of external business partners. The report does not include control or supervision with subcontractors in relation to Cloud-based ERP system. These subcontractors are listed in detail in Data Processing Agreements with the customers.

The scope of our report does not cover customer-specific conditions, and the report does not include the complementary controls and control activities conducted by the user company; see the description of the company in Chapter 2 (incl. Appendix 1) under the section: Customers' responsibilities (complementary controls at the customer).

Uniconta A/S' responsibility

Uniconta A/S is responsible for the preparation of the description and accompanying assertion in Chapter 2 (including Appendix 1), including the completeness, accuracy and method of presentation of the description and assertion; for providing the services covered by the description; for stating the control objectives; and for designing, implementing and effectively operating controls to achieve the stated control objectives.

Beierholm's independence and quality management

We have complied with the requirements of independence and other ethical requirements laid down in FSR's Ethical Rules based on fundamental principles of integrity, objectivity, professional competence and requisite care, confidentiality and professional conduct.

We apply ISQC 1 and thus sustain a comprehensive system of quality management, including documented policies and procedures for compliance with ethical rules, professional standards as well as requirements in force under existing laws and additional regulation.

Auditor's responsibility

Our responsibility is to express an opinion, based on our procedures, on Uniconta A/S' description and on the design and operation of controls related to the control objectives stated in the said description. We have conducted our engagement in accordance with ISAE 3402, Assurance Reports on Controls at a Service Organisation, issued by the IAASB. The standard requires that we comply with ethical requirements and that we plan and perform our procedures to obtain reasonable assurance about whether, in

all material respects, the description is fairly presented, and whether the controls in all material aspects are appropriately designed and operate effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and about the design and operating effectiveness of controls. The procedures selected depend on the judgement of the service organisation's auditor, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or not operating effectively.

Our procedures included testing the operating effectiveness of such controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description have been achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified and described by Uniconta A/S in Chapter 2 (including Appendix 1).

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

Limitations of controls at Uniconta A/S

Uniconta A/S' description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in their own particular environment. Moreover, because of their nature, controls at Uniconta A/S may not prevent or detect all errors or omissions in processing or reporting transactions. Furthermore, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at the service organisation may become inadequate or fail.

Opinion

Our opinion is based on the matters outlined in this report. The criteria on which our opinion is based are those described in Chapter 1 under Letter of Representation. In our opinion,

a) The description fairly presents control environment for the operation of the Cloud-based ERP system, such as this control environment was designed and implemented throughout the period 1 December 2019 - 30 November 2020 in all material respects; and

b) The controls related to the control objectives stated in the description were in all material respects suitably designed throughout the period 1 December 2019 - 30 November 2020; and

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved in all material respects, had operated effectively throughout the period 1 December 2019 - 30 November 2020.

Description of tests of controls

The specific controls tested and the nature, timing and findings of those tests are listed in Chapter 4.

Intended users and purpose

This report and the description of the test of controls in Chapter 4 are solely intended for Uniconta A/S' customers and their auditors, who have sufficient understanding to consider them along with other information, including information about the customers' own control measures, which the customers i.e. the Data Controllers themselves have performed, when assessing compliance with the demands to the control environment as well as with requirements of the General Data Protection Regulation.

Søborg, 11 December 2020

Beierholm
State Authorized Public Accountants
CVR 32 89 54 68

Kim Larsen
State-authorized Public Accountant

Jesper Aaskov Pedersen
IT-auditor, Manager

CHAPTER 4:

Auditor's description of control objectives, security measures, tests and findings

We have structured our engagement in accordance with ISAE 3402 – Assurance Reports on Controls at a Service Organisation. For each control objective, we start with a brief summary of the control objective as described in the frame of reference ISO27001 and 27002.

With respect to the period, we have tested whether Uniconta A/S has complied with the control objectives throughout the period 1 December 2019 - 30 November 2020.

Below the grey field are three columns:

- **The first column tells the activities Uniconta A/S, according to its documentation, has put into practice in order to comply with the requirements.**
- **The second column tells how we have decided to test, whether facts tally with descriptions.**
- **The third column tells the findings of our test.**

The Tests Performed

The tests performed in connection with establishing the control measures' design, implementation and operational efficiency are conducted using the methods described below:

Inspection	**Reading of documents and reports containing information about execution of the control. This includes, inter alia, reading and deciding about reports and other documentation in order to asses, whether it can be expected that the design of specific control measures will be efficient, if implemented. Furthermore, it is assessed, whether control measures are monitored and controlled sufficiently and with appropriate intervals.**
Enquiries	**Enquiries to/interview with relevant staff at Uniconta A/S. Enquiries have included how control measures are performed.**
Observation	**We have observed the performance of the control.**
Repeating the control	**Repeated the relevant control measure. We have repeated the performance of the control in order to verify that the control measure works as assumed.**

CONTROL OBJECTIVE - INTRODUCTION:

Risk Assessment and Management

The risk assessment must identify and prioritise the risks based on the operation of Cloud-based ERP system. The findings are to contribute to the identification and prioritisation of management interventions and precautionary measures necessary to address relevant risks.

Uniconta A/S' control procedures	Auditor's test of controls	Test findings
Through a risk assessment, risks have been identified and prioritised. The Cloud-based ERP system defined in the description is used as basis for the assessment. **The findings contribute to the identification and prioritisation of management interventions and precautionary measures necessary to address relevant risks.**	**We have requested and obtained the relevant material in connection with the audit of risk management.** **We have checked that regular risk assessments are carried out for the Cloud-based ERP system in relation to business conditions and their development. We have checked that the risk assessment is deployed down through the company's organisation.** **We have checked that the company's exposure is managed on a current basis and that relevant adaptations of consequences and probabilities are made regularly.**	**During our test, we did not identify any material deviations.**

CONTROL OBJECTIVE 5:

Information Security Policies

Management must prepare an information security policy that covers, among other things, management's security objectives, policies and overall action plan. The information security policy will be maintained, taking the current risk assessment into consideration.

Uniconta A/S' control procedures	Auditor's test of controls	Test findings
There is a written strategy covering, among other things, Management's security objectives, policies and overall action plan. The IT security policy and accompanying supporting policies are approved by the company's Management, and then deployed down through the company's organisation. The policy is available for all relevant employees. The policy is re-evaluated according to planned intervals.	We have obtained and audited Uniconta A/S' latest IT security policy. During our audit, we checked that maintenance of the IT security policy is conducted on a regular basis. At the same time, we checked during our audit that the underlying supporting policies have been implemented. We have checked that the policy is approved and signed by the company's Supervisory and Executive Boards and made available for the employees on Uniconta A/S' intranet.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 6:

Organisation of Information Security

Management of the IT security must be established in the company. Organisational responsibility for the IT security must be placed with appropriate business procedures and instructions. The person responsible for IT security must, among other things, ensure compliance with security measures, including continuous updating of the overall risk assessment.

Uniconta A/S' control procedures	Auditor's test of controls	Test findings
Organisational responsibility for IT security has been placed, documented and implemented. **The IT security has been coordinated across the company's organisation.**	**Through inspection and tests, we have ensured that the organisational responsibility for IT security is documented and implemented.** **We have checked that the IT security is deployed across the organisation in relation to cloud-based ERP system.** **By making interviews, we have checked that the person responsible for IT security knows his/her role and responsibilities.**	**During our test, we did not identify any material deviations.**

CONTROL OBJECTIVE 7:

Human Resource Security

It must be ensured that all new employees are aware of their specific responsibilities and roles in connection with the company's information security in order to minimise the risk of human errors, theft, fraud and abuse of the company's information assets.

Uniconta A/S' control procedures	Auditor's test of controls	Test findings
Based on the specified work processes and procedures, it is ensured that all new employees are informed of their specific responsibilities and roles in connection with their employment at Uniconta A/S. This includes the framework laid down for the work and the IT security involved. Security responsibilities, if any, are determined and described in job descriptions and in the form of employment contract terms. The employees are familiar with their professional secrecy based on a signed employment contract and through Uniconta A/S' HR policy.	We have verified that routines and procedures developed by Management in connection with start of employment and termination of employment have been adhered to. Based on random samples, we have tested whether the above routines and procedures have been complied with in connection with start of employment and termination of employment. Through interviews, we have checked that employees of significance to Cloud-based ERP system are familiar with their professional secrecy. We have examined the job descriptions and employment contracts of key employees and subsequently tested the awareness of the individual employee of their roles and related security responsibility. We have ensured that Uniconta A/S' HR policy is easily accessible and has a section on terms for professional secrecy with respect to information obtained in connection with work conducted at Uniconta A/S.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 8:

Asset Management

Necessary protection of the company's information assets must be ensured and maintained, all the company's physical and functional assets related to information must be identified, and a responsible owner appointed. The company must ensure that information assets related to cloud-based ERP system have an appropriate level of protection.

There must be reassuring controls to ensure that data media are properly disposed of when no longer needed, in accordance with formal procedures.

Uniconta A/S' control procedures	Auditor's test of controls	Test findings
All information assets have been identified and an updated list of all significant assets has been established. An "owner" of all significant assets is appointed in connection with the operation of Cloud-based ERP system.	We have examined and checked the company's central IT register for significant IT entities in connection with the operation of Cloud-based ERP system. Through observations and control, we checked relations to central knowhow systems for the operation of Cloud-based ERP system. By observations and enquiries, we have checked that Uniconta A/S complies with all material security measures for the area in accordance with the security standard.	During our test, we did not identify any material deviations.
Information and data in relation to Cloud-based ERP system are classified based on business value, sensitivity and need for confidentiality.	We have controlled that there is an appropriate division of assets and accompanying procedures/routines in relation to Uniconta A/S' services. In this connection, we have controlled, whether internal procedures/routines regarding ownership to applications and data are complied with. We have checked that contracts and SLA are used as central tools to ensure the definition, segregation and delimitation of Uniconta A/S' responsibilities and the customer's responsibilities with respect to access to information and data. Accordingly, the customer is typically responsible for ensuring that a suitable protection level exists for own information and data.	During our test, we did not identify any material deviations.
Procedures for dealing with destruction of data media are established.	We have: · Asked Management which procedures/ control activities are performed regarding data media. · On a sample basis gone through the procedures for destruction of data media.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 9:

Access Control

Access to the company's systems, information and network must be controlled based on business and statutory requirements. Authorised users' access must be ensured, and unauthorised access must be prevented.

Uniconta A/S' control procedures	Auditor's test of controls	Test findings
Documentation and updated directions exist for Uniconta A/S' access control.	We have: · asked Management whether access control procedures have been established at Uniconta A/S. · verified on a test basis that access control procedures exist and have been implemented; see Uniconta A/S' directions. · by interviewing key staff and by inspection on a test basis, we have verified that access control for the operations environment comply with Uniconta A/S' directions, and authorisations are granted according to agreement.	During our test, we did not identify any material deviations.
A formal business procedure exists for granting and discontinuing user access. Granting and application of extended access rights are limited and monitored.	We have asked Management, whether access control procedures have been established at Uniconta A/S. We have by inspection on a test basis verified: · that adequate authorisation systems are used in relation to access control at Uniconta A/S. · that the formalised business procedures for granting and discontinuing user access have been implemented in Uniconta A/S' systems, and registered users are subject to regular follow-up.	During our test, we did not identify any material deviations.
Internal users' access rights are reviewed regularly according to a formalised business procedure.	By inspection on test basis, we have verified that a formalised business procedure exists for follow-up on authorisation control according to the directions, including: · that formal management follow-up is performed on registered users with extended rights every 3 months. · that formal management follow-up is performed on registered users with ordinary rights every 6 months.	During our test, we did not identify any material deviations.

The granting of access codes is controlled through a formalised and controlled process, which ensures, among other things, that standard passwords are changed.	**We have asked Management whether procedures granting access code have been established at Uniconta A/S.** **By inspection on a test basis, we have verified** · **that an automatic systems control takes place, when access codes are granted to check that passwords are changed after first login.** · **that standard passwords are changed in connection with implementation of systems software, etc.** · **if this is not possible, that procedures ensure that standard passwords are changed manually.**	**During our test, we did not identify any material deviations.**
Access to operating systems and networks are protected by passwords. **Quality requirements have been specified for passwords, which must have a minimum length (7 characters), requirements as to complexity, maximum duration (max 42 days), and likewise password setup means that passwords cannot be reused.**	**We have asked Management whether procedures ensuring quality passwords in Uniconta A/S are established.** **By inspection on a test basis, we have verified that appropriately programmed controls have been established to ensure quality passwords complying with the policies for:** · **minimum length of password** · **complexity of password** · **minimum life of password** · **maximum life of password** · **minimum history of password**	**During our test, we did not identify any material deviations.**

CONTROL OBJECTIVE 12:

Operations Security

Control objective: Operations procedures and areas of responsibility.

A correct and adequate running of the company's operating systems must be ensured. The risk of technology related crashes must be minimised. A certain degree of long-term planning is imperative in order to ensure sufficient capacity. A continuous capacity projection must be performed based on business expectations for growth and new activities and the capacity demands derived hereof.

Uniconta A/S' control procedures	Auditor's test of controls	Test findings
The operations procedures for business-critical systems are documented, and they are available to staff with work-related needs. Management has implemented policies and procedures to ensure satisfactory segregation of duties.	We have: · Asked Management whether all relevant operation procedures are documented. · In connection with our audit of the individual areas of operation verified on a test basis that documented procedures exist and that there is concordance between the documentation and the procedures actually performed. · Inspected users with administrative rights in order to verify that access is justified by work-related needs and does not compromise the segregation of duties.	During our test, we did not identify any material deviations.
Management of operational environment is established in order to minimise the risk of technology related crashes. Continuous capacity projection is performed based on business expectations for growth and new activities and the capacity demands derived hereof.	We have: Asked Management about the procedures and control activities performed. On a test basis examined that the operation environment's consumption of resources is monitored and adapted to the expected and necessary capacity requirements.	During our test, we did not identify any material deviations.

Control objective: Protection from malware

To protect from malicious software, such as virus, worms, Trojan horses and logic bombs. Precautions must be taken to prevent and detect attacks from malicious software.

Uniconta A/S' control procedures	Auditor's test of controls	Test findings
Preventive, detecting and remedial security and control measures have been established, including the required training and provision of information for the company's users of information systems against malicious software.	We have: · enquired about and inspected the procedures/ control activities performed in the event of virus attacks or outbreaks. · enquired about and inspected the activities meant to increase the employees' awareness of precautions against virus attacks or outbreaks. · verified that anti-virus software has been installed on servers and inspected signature files documenting that they have been updated.	During our test, we did not identify any material deviations.

Control objective: Back-up

To ensure the required accessibility to the company's information assets. Set procedures must be established for back-up and for regular testing of the applicability of the copies.

Uniconta A/S' control procedures	Auditor's test of controls	Test findings
Backup is made of all of the company's significant information assets, including, e.g. parameter setup and other operations-critical documentation, according to the specified directions.	We have: · asked Management about the procedures/ control activities performed. · examined backup procedures on a test basis to confirm that these are formally documented. · examined backup log on a test basis to confirm that backup has been completed successfully and that failed backup attempts are handled on a timely basis. · examined physical security (e.g. access limitations) for internal storage locations to confirm that backup is safely stored.	During our test, we did not identify any material deviations.

Control objective: Logging and monitoring

To reveal unauthorised actions. Business-critical IT systems must be monitored, and security events must be registered. Logging must ensure that unwanted incidences are detected.

Uniconta A/S' control procedures	Auditor's test of controls	Test findings
Operating systems and network transactions or activities involving special risks are monitored. Abnormal conditions are examined and resolved on a timely basis. Uniconta A/S logs, when internal users log off and on the systems. Only in the event of suspected or identified abuse of the systems, users are actively monitored.	We have: · asked Management about the procedures/ control activities performed, and have examined the system setup on servers and important network units as well as verified that parameters for logging have been set up, thus transactions made by users with extended rights are being logged. · checked on a test basis that logs from critical systems are subject to sufficient follow-up.	During our test, we did not identify any material deviations.
A central monitoring tool is used which sends alerts, if known errors occur. If possible, it is monitored whether an error is about to occur in order to react proactively. Alerts are shown on the monitoring screen mounted in the project and operations department. Critical alerts are also sent by email and SMS. Status reports are sent by email from different systems. Some daily – others when incidents occur in the system. The operation function is responsible for checking these emails daily.	We have: · asked Management about the procedures/ control activities performed. · ensured that a monitoring tool is used and that this is available to all employees. · ensured that alerts are sent by email and SMS, if errors occur. · examined status reports. · ensured that an operations function is established and that this function checks reports on a daily basis.	During our test, we did not identify any material deviations.

Control objective: Managing operations software and managing vulnerability

Ensuring establishment of appropriate procedures and controls for implementation and maintenance of operating systems.

Uniconta A/S' control procedures	Auditor's test of controls	Test findings
Changes in the operation environment comply with established procedures.	We have asked Management, whether procedures for patch management are established in Uniconta A/S. By inspection on test basis, we have verified that · adequate procedures are applied, when controlled implementation of changes to the production environment of Uniconta A/S is performed. · changes to Uniconta A/S' operation environment comply with directions in force, including correct registration and documentation of applications about changes. On a test basis, we have inspected that the operating systems are updated in compliance with procedures in force and that current status is registered.	During our test, we did not identify any material deviations.
Changes in existing user systems and operation environments comply with formalised procedures and processes.	We have asked Management, whether procedures for patch management are established in Uniconta A/S. By inspection on test basis, we have verified that adequate procedures are applied for controlled implementation of changes in the production environments, including that demands to the patch management controls ensure that · applications for change are registered and described. · all changes are subject to formal approval before implementation · changes are subject to formal impact assessments. · fall-back plans are described. · systems affected by changes are identified. · documented test of changes is performed before implementation · documentation is updated reflecting the implemented changes in all material respects. · procedures are subject to managing and coordination in a "change board".	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 13:

Communication Security

To ensure protection of information in networks and support of information processing facilities.

Uniconta A/S' control procedures	Auditor's test of controls	Test findings
Networks must be protected against threats in order to secure network-based systems and the transmitted data. Production environment must be secured against failing supply in relation to redundancy to network connection to the internet. Network traffic/access from production environment to the outside world is available by means of multiple supply entries or access from more than one supplier.	It has been checked that necessary protection against unauthorised access is implemented, including: · Appropriate procedures for managing network equipment are established. · Segregation of user functions is established. · Appropriate logging and monitoring procedures are established. · Managing the company's network is coordinated in order to ensure optimal utilisation and a coherent security level. · Ensured that connections for data communication with the internet are established via more than one ISP supplier. · On a sample basis gone through documentation from the suppliers about written basis for contract, as well as regular settlement of accounts for services rendered by the ISP suppliers.	During our test, we did not identify any material deviations.
Adequate procedures for managing threats in the form of attacks from the internet (cyber-attacks) must be implemented. In this connection, tools for managing the contingency approach in the event of a cyber-attack must be devised.	We have controlled that an adequate number of procedures with accompanying contingency plans regarding managing threats in relation to cyber-attacks are implemented. We have by inspection on a test basis ensured · that appropriate framework for managing cyber-attacks are devised. · that plans for managing the threat are devised and implemented. · that the plans include cross-organisational collaboration between internal groups.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 14:

System acquisition, development and maintenance

Ensure that software development related to Cloud-based ERP-system solutions is managed using suitable IT control measures, including appropriate segregation between production and development environment.

Uniconta A/S' control procedures	Auditor's test of controls	Test findings
Uniconta A/S has planned system development and maintenance activities based on the proprietary model for project management. All changes meant to be put into operation in the production environment, must be approved by the development group.	We have checked the existence of formal procedures and work routines for segregation between production and development. User management ensures suitable control measures in connection with managing the logical access control. We have checked that the different user groups are controlled at set intervals. The structure of the development organisation includes a central steering committee responsible for providing suitable work routines and accompanying control measures for the management. In connection with our audit, we have checked that internal education is conducted for staff working with Cloud-based ERP system and the accompanying development environment. During the process we tested, whether staff was trained in using Uniconta A/S' quality model for development. The control environment for the development platform is based on the same IT security structure as stated for the production environment. All user activities are recorded and logged in the central database. The person responsible for IT security reviews the log database on a regular basis.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 15:

Supplier Relationships

External business partners are obliged to comply with the company's established framework for IT security level.		
Uniconta A/S' control procedures	**Auditor's test of controls**	**Test findings**
Risks related to external business partners are identified, and security agreements is managed.	We have verified that in connection with the use of external business partners there are formal cooperation agreements. On a test basis, we have inspected that the cooperation agreements with external suppliers comply with the requirements about covering relevant security conditions in relation to the individual agreement.	During our test, we did not identify any material deviations.
In case of changes with impact on the production environment, and where services from external suppliers are used, suppliers are selected by the IT Security Manager. Solely recognised suppliers are used.	We have asked Management about relevant procedures applied in connection with choosing external partners. We have ensured that appropriate procedures for managing cooperation with external partners are established. We have tested that key suppliers have updated and approved contracts.	During our test, we did not identify any material deviations.
Monitoring must be conducted on a regular basis, including supervision of external business partners.	We have ensured that there are appropriate processes and procedures for ongoing monitoring of external suppliers. We have checked that ongoing supervision is conducted by means of independent auditor's reports.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 16:

Information Security Incident Management

To achieve reporting of security incidents and weaknesses in the company's information processing systems in a way that allows for timely corrections.

Uniconta A/S' control procedures	Auditor's test of controls	Test findings
Security incidents are reported to Management as soon as possible, and the handling is performed in a consistent and efficient way.	We have asked Management whether procedures are established for reporting security incidents. We have verified that procedures and routines are developed for reporting and handling of security incidents, and that the reporting is submitted to the right places in the organisation; see the directions. We have verified that the responsibility for the handling of critical incidents is clearly delegated, and that the related routines ensure that security breaches are handled expediently, efficiently and methodically.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 17:

Information Security Aspects of Business Continuity Management

Business continuity management is to counteract interruption in the company's business activities, protect critical information assets against the impact of a major crash or disaster, as well as ensure fast recovery.

Uniconta A/S' control procedures	Auditor's test of controls	Test findings
A consistent framework has been established for the company's contingency plans to ensure that all the plans are coherent and meet all security requirements and to determine the prioritisation of tests and maintenance.	We have asked Management whether business continuity management has been developed for Cloud-based ERP system at Uniconta A/S. By inspection on a test basis, we have verified · that appropriate framework for preparation of business continuity management has been established · that contingency plans are prepared and implemented · that the plans include business continuity management across the organisation · that the plans include appropriate strategy and procedures for communication with the stakeholders of Uniconta A/S. · that contingency plans are tested on a regular basis · that maintenance and reassessment of the total basis for business continuity management is undertaken on a regular basis.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 18:

Compliance with the Role as Data Processor

Principles for processing personal data:

Procedures and controls are complied with to ensure that collecting, processing and storing of personal data are performed in accordance with the agreements for processing personal data.

Uniconta A/S' control procedures	Auditor's test of controls	Test findings
A uniform framework is established in the form of standard contracts, Service Level Agreements, as well as Data Processor Agreements or the like, containing an outline of the basis for processing personal data.	We have controlled the existence of updated procedures in writing for processing personal data, and that the procedures include requirements to legal processing of personal data.	During our test, we did not identify any material deviations.
Personal data is only processed according to directions from the Data Controller.	We have controlled that Management secures that personal data is only processed according to directions. We have controlled by a random check of a suitable number of processings that these are conducted according to directions.	During our test, we did not identify any material deviations.
Management immediately informs the Data Controller, if a direction, in the Data Processor's opinion, infringes the GDPR or the data protection rules according to other EU or member state data protection provisions.	We have controlled that Management secures that processing is examined, and that formalised procedures exist ensuring verification that processing is not against the GDPR or other legislation. We have controlled that procedures are in place for informing the Data Controller of cases where the processing of personal data is evaluated to be against legislation. We have controlled that the Data Controller was informed in cases, where the processing of personal data was evaluated to be against legislation.	During our test, we did not identify any material deviations.

Data processing: Procedures and controls are complied with to ensure that personal data can be deleted or returned if arrangements are made with the data controller to this effect.		
Uniconta A/S' control procedures	**Auditor's test of controls**	**Test findings**
Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the Data Controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have controlled that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the Data Controller. We have controlled that the procedures are up to date.	During our test, we did not identify any material deviations.
Upon termination of the processing of personal data for the Data Controller, data has, in accordance with the agreement with the Data Controller, been: · Returned to the Data Controller; and/or · Deleted if this is not in conflict with other legislation.	We have controlled that formalised procedures are in place for processing the Data Controller's data upon termination of the processing of personal data. We have controlled by using a suitable random sample of terminated data processing sessions during the assurance period that documentation exists that the agreed deletion or return of data has taken place.	During our test, we did not identify any material deviations.
Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the Data Controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have controlled that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements. We have controlled that the procedures are up to date. We have controlled by way of random samples, whether underlying documentation exist in connection with data processing ensuring that data processing takes place in accordance with the data processing agreement.	During our test, we did not identify any material deviations.

The Data Processor's responsibility: Procedures and controls are complied with to ensure that only approved sub-processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of Data Subjects and the processing of personal data, the Data Processor ensures adequate security of processing.		
Uniconta A/S' control procedures	**Auditor's test of controls**	**Test findings**
Written procedures exist which include requirements for the data processor when using sub-processors, including requirements for sub-processing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have controlled that formalised procedures are in place for using sub-processors, including requirements for sub-processing agreements and instructions. Inspected that procedures are up to date.	During our test, we did not identify any material deviations.
The Data Processor only uses sub-processors to process personal data that have been specifically or generally approved by the Data Controller.	Inspected that the Data Processor has a complete and updated list of sub-processors used. Inspected by way of a sample of 1 sub-processor from the Data Processor's list of sub-processors that documentation exists that the processing of data by the sub-processor is stated in the data processing agreement – or otherwise approved by the Data Controller.	During our test, we did not identify any material deviations.
When changing the generally approved sub-processors used, the Data Controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the Data Processor. When changing the specially approved sub-processors used, this has been approved by the Data Controller.	We have controlled that formalised procedures are in place for informing the Data Controller when changing the sub-processors used. Inspected documentation that the Data Controller was informed when changing the sub-processors used throughout the assurance period.	During our test, we did not identify any material deviations.
The Data Processor has subjected the sub-processor to the same data protection obligations as those provided in the data processing agreement or similar document with the Data Controller.	Checked by way of inspection for existence of signed sub-processing agreements with sub-processors used, which are stated on the Data Processor's list. Inspection by way of a sample of 1 sub-processing agreement that they include the same requirements and obligations as are stipulated in the data processing agreements between the Data Controllers and the Data Processor.	During our test, we did not identify any material deviations.

The Data Processor has a list of approved sub-processors disclosing: · **Name;** · **Business Registration No. (CVR-no.);** · **Address;** · **Description of the processing.**	**We have controlled that the Data Processor has a complete and updated list of sub-processors used and approved.** **Inspected that, as a minimum, the list includes the required details about each sub-processor.**	**During our test, we did not identify any material deviations.**

Assisting the Data Controller: **Procedures and controls are complied with to ensure that the Data Processor can assist the Data Controller in handing out, correcting, deleting or restricting information on the processing of personal data to the Data Subject.**		
Uniconta A/S' control procedures	**Auditor's test of controls**	**Test findings**
Written procedures exist which include a requirement that the Data Processor must assist the Data Controller in relation to the rights of Data Subjects. **Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.**	**We have controlled that formalised procedures are in place for the Data Processor's assistance to the Data Controller in relation to the rights of Data Subjects.** **Inspected that procedures are up to date.**	**During our test, we did not identify any material deviations.**
The Data Processor has established procedures in so far as this was agreed that enable timely assistance to the Data Controller in handing out, correcting, deleting or restricting or providing information about the processing of personal data to Data Subjects.	**We have controlled that the procedures in place for assisting the Data Controller include detailed procedures for:** · **Handing out data;** · **Correcting data;** · **Deleting data;** · **Restricting the processing of personal data;** · **Providing information about the processing of personal data to Data Subjects.** **Inspected documentation that the systems and databases used support the performance of the relevant detailed procedures.**	**During our test, we did not identify any material deviations.**

Records of processing activities: Procedures and controls are complied with to ensure that the Data Processor keeps records of processing personal data for which the Data Processor is responsible.		
Uniconta A/S' control procedures	**Auditor's test of controls**	**Test findings**
Records exist of processing activities for the Cloud-based ERP system in combination with the relevant Data Controller.	We have controlled documentation displaying the existence of records for processing activities for the Cloud-based ERP system combined with the relevant Data Controller.	During our test, we did not identify any material deviations.
Assessments are made on a regular basis – and at least once a year - as to whether the records are updated and correct.	We have controlled the documentation disclosing that the records of the processing activities for each Data Controller are updated and correct.	During our test, we did not identify any material deviations.

Reporting breaches of personal data security to the Supervisory Authority (the Danish Data Protection Agency): Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.		
Uniconta A/S' control procedures	**Auditor's test of controls**	**Test findings**
Written procedures exist – updated at least once a year - describing how to manage personal data security breaches, including a requirement of timely communication to the Data Controllers.	We have controlled that updated written procedures for managing data security breaches exist, including that timely communication to the Data Controller is described.	During our test, we did not identify any material deviations.
The Data Processor ensures recording of all personal data security breaches.	We have controlled documentation disclosing that all personal data security breaches are recorded at the Data Processor.	During our test, we did not identify any material deviations.
Management has ensured that all personal data security breaches are timely and sufficiently communicated to the Data Controller, including personal data security breaches happened at Data Processors used as subcontractors.	We have controlled documentation displaying that Management has ensured that all personal data security breaches are timely and sufficiently communicated to the Data Controller, including personal data security breaches happened at Data Processors used as subcontractors.	During our test, we did not identify any material deviations.