

JANUARY 2025

## INVENTIO.IT A/S

ISAE 3402 TYPE II ASSURANCE REPORT

CVR 26112001

Independent auditor's Report on the control environment in relation to IT operation of ERP Online Services.

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**  
**Godkendt Revisionspartnerselskab**  
**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](http://www.beierholm.dk)



# Structure of the Assurance Report

## Chapter 1:

Letter of Representation.

## Chapter 2:

Description of the control environment in relation to the IT operation of ERP Online Services.

## 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


Inventio.IT A/S processes personal data on behalf of customers according to Data Processor Agreements regarding IT operation of ERP Online Services.

The accompanying description has been prepared for the use of customers and their auditors, who have used Inventio.IT A/S' ERP Online Services, 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.

Inventio.IT A/S hereby confirms that

(A) The accompanying description, Chapter 2 (incl. Appendix 1) gives a true and fair description of Inventio.IT A/S' control environment in relation to IT operations of ERP Online Services throughout the period 1 January 2024 - 31 December 2024. 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 is 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 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 the IT operation of ERP Online Services – 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 the IT operation of ERP Online Services performed throughout the period 1 January 2024 - 31 December 2024
- (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 January 2024 - 31 December 2024. 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 January 2024 - 31 December 2024.
- (C) Appropriate technical and organizational security measures are established in order to honour the agreements with the Data Controllers, 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 Inventio.IT A/S' standard agreement as well as related Data Processing Agreement. The criteria for this basis are:
  - (i) Inventio.IT – Service Level Agreement
  - (ii) Inventio.IT – Data Processor Agreement

Brøndby, 9 January 2025

**Michael Steen Sørensen**  
CEO

**Kenneth Kornbeck Lindeblad**  
IT Security Coordinator/ Marketing Manager

Inventio.IT A/S, Vallensbæksvej 45, DK-2605 Brøndby, CVR 26112001

# Description of control environment in connection with IT operation of ERP Online Services

## Introduction

The purpose of this description is to provide Inventio.IT 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 exposure of the technical and organizational security measures implemented in connection with the IT operation of Inventio.IT A/S' ERP Online Services.

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.

## The scope of this description

Inventio.IT is a provider of IT services online services within ERP, and Inventio.IT's core activity is ERP Online Services, which include development and delivery of standardised online solutions for Microsoft Dynamics' series of products. Monitoring and support are on Inventio.IT's own platform placed in Inventio.IT's data center.

As provider Inventio.IT is responsible for establishing and maintaining appropriate procedures and control measures with the purpose of finding and preventing errors, in order to meet the requirements laid down in the agreements. It is this core activity that is the basis for the present description.

## Description of Inventio.IT A/ S


Inventio.IT A/S was established in 2001 and is a sound Danish business enterprise with stable growth and profit. In 2019 we became part of the listed Swedish Dustin Group.

Our strength is standardised and subscription-based ERP solutions for Microsoft Dynamics, but we also develop customized solutions (Extensions) for customers, who have such needs. Trust and confidence are the key-words when selecting business partners, and that is why our emphasis at Inventio.dk is on maintaining an organization where all employees are competent, experienced, reliable, and with great commitment to each customer.

We are about 60 employees, and due to our units on Zealand and in Jutland we cover the whole country. We focus on small and medium-sized enterprises, as we can use all our competences in the best way in this segment. We also serve our international customers' subsidiaries and sister companies in, inter alia, Scandinavia, Europe, Africa, and North America.

## Business strategy / IT security strategy

It is still Inventio.IT's strategy to exploit our expertise within hosting of ERP systems and to further develop online services for sale via a subscription-based model in large volumes.



Our future-oriented solutions for Microsoft Dynamics 365 help small and medium-sized enterprises, who want to exploit the possibilities of ERP in the Cloud by moving from an outdated platform with limited possibilities and to start automizing and optimizing in a cheap and easy way.

We differ from the traditional ERP provider, as we offer price-efficient online services (SMART apps) covering the demand for a fast and easy way of starting the process of standardising and efficiency improvements of business conduct, typical processes, and collaboration - both internally in their own business and externally with their customers.

With our online services for ERP (SMART apps and online platform), we are already a leader within volume sales of Microsoft ERP Systems. With the help of our expertise about ERP and hosting, this market must be extended. With further development of present products as well as with addition of new products.

### Hosted ERP solutions

Inventio.IT offers the following ERP Online Services:

- ERP-online SMART apps  
(BOnline, NAVonline, C5online)

Inventio.IT is working with IT security at a business-strategic level, and on this background works on a continuous basis to ensure a high level of service and quality. Both Inventio.IT's own management and Dustin Group, who is the owner of Inventio.IT, give IT security a high priority as an important part of the company's business culture, by means of the company's security policy.

Inventio.IT A/S has decided to base its IT security strategy on ISO27001 + 2 and is thus applying the ISO methodology to implement relevant security measures within the following areas:

- |   |  |
|---|--|
| <ul style="list-style-type: none"><li>• Information security policy</li><li>• Organisation of information security</li><li>• Human resource security</li><li>• Asset management</li><li>• Access control</li><li>• Cryptography</li><li>• Physical and environmental security</li><li>• Operations security</li><li>• Communications security</li></ul> | <ul style="list-style-type: none"><li>• Acquisition, development, and maintenance of systems</li><li>• Supplier relationships</li><li>• Information security incident management</li><li>• Information security aspects of business continuity management</li><li>• Compliance with legal and contractual requirements</li></ul> |
|---|--|

The control objectives and security measures implemented by Inventio.IT A/S are listed in Appendix 1 to this description.

### Inventio.IT A/ S' organisation and organising of IT security

Inventio.IT's formal responsibility for IT security and procedures is placed at the CSO/CEO. The company's Board of Directors approves the IT security policy.

At Inventio.IT there is a clearly divided organization in relation to responsibility, and Inventio.IT has comprehensive descriptions of responsibility and roles at all levels, from management to each employee in operations.

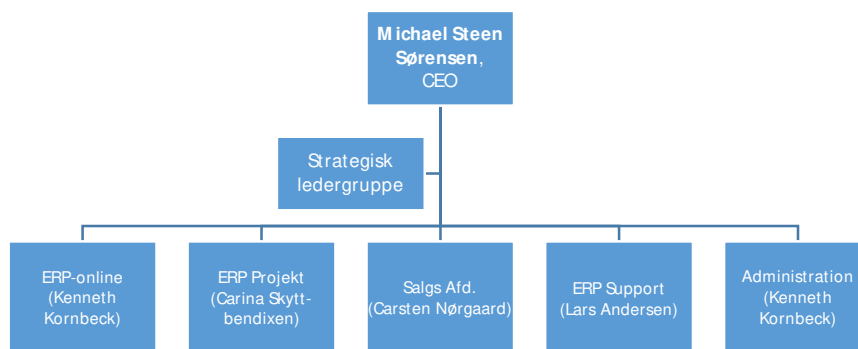
On an ongoing basis, all employees are kept updated about changes in the IT security policy. Coordination of information and training is planned by the IT security coordinator.

When using external business partners, a collaboration agreement is devised before the start of any work.

Inventio.IT's organization is divided into 5 departments – ERP Online, ERP Support, ERP Project, Sales, and Administration.

As most of the requirements regarding IT security are related to ERP Online, Kenneth Kornbeck Lindeblad takes on the role as IT security coordinator across all departments.

This is the reason, we place emphasis on running an organization solely including employees, who are competent, experienced, reliable, and with great commitment to each customer.



We focus on the business objectives and requirements of each company, and we take pride in complying with deadlines, budgets, functionality, and quality.

We have a flat organizational structure, where the step from decision to action is a short one, and where all employees are working with development as well as with serving our customers.

Our reputation is "Once customer at Inventio.IT – always customer at Inventio.IT". There is something similar going on with our employees, and many of them have been working with us from our start in 2001. All this develops very good relations between us and our customers. We take pride in having a staff, who is content and is updated on a continuous basis via courses etc. At present we have several Microsoft certifications, and we are a Microsoft Gold Partner.

### **Risk management at Inventio.IT A/ S**


It is Inventio.IT's policy that the risks connected with our company's activities are covered or limited to a level allowing the company to maintain normal operations. Inventio.IT conducts risk management and internal controls in several areas and on several levels. We perform an annual risk and threat assessment.

Inventio.IT has implemented set procedures for risk assessment of our business and particularly of ERP Online. In this way, we ensure that the risks related to the services we provide, are minimized to an acceptable level. Risk assessment is conducted regularly, as well as when we make changes to existing systems or implement new systems, which we consider relevant in connection with re-assessing our overall risk assessment. The responsibility for the risk assessment is placed at the CEO.

As part of the IT security strategy mentioned above, Inventio.IT works with the international standard for IT security – ISO27001+2 – constituting the primary framework for the IT security. The IT security work process is a continuous and dynamic process ensuring that Inventio.IT all the time lives up to our customers' requirements and needs.

### **Managing IT security**

The management of Inventio.IT has the day-to-day responsibility for IT security, and it is in this way ensured that the overall requirements and framework for IT security are maintained. Management has



described Inventio.IT's structure for IT security by means of the overall IT security policy. The IT security policy must as a minimum be revised once a year.

The definition of Inventio.IT's quality management system is based on the general objective of providing stable and secure IT operations for our customers. In order to fulfil this objective, it has been necessary to implement policies and procedures ensuring that our deliveries are uniform and transparent.

Inventio.IT's IT security policy has been prepared with reference to the items mentioned above and applies to all employees and all deliveries. In case of an error or security breach in our operating environment, the error/security breach is rectified immediately.

All servers and network units are documented in Inventio.IT's documentation system. All changes in our system are logged here.

The security policy establishes the fundamental policies for Inventio.IT's infrastructure and does not include conditions in relation to specific products, services, or users.

The security policy is providing Inventio.IT with one common set of rules. In this way, we achieve a stable operating environment and a high security level. We make regular improvements to policies, procedures, and operations.

In the area of overall IT security, Inventio.IT has implemented the necessary procedures and control measures relating to each of the areas within ISO27001+2 as defined in Appendix 1, showing the security structure and the control objectives implemented at Inventio.IT.

### **HR, employees, and training**

Everybody at Inventio.IT must meet the requirements of the role they have been given and comply with our procedures - see our IT security policy. This is, inter alia, to ensure that security issues are adapted and managed. At Inventio.IT, top priority is always applied to securing the customers' data, the company's equipment - and in this way - the business itself.

Description of roles and responsibilities, including tasks and responsibilities in relation to security, are defined in the devised role descriptions, the staff's employment contracts, as well as in the IT security policy.

The general terms and conditions of the employment include that the employee all the time is subject to the applicable IT security policy.

Inventio.IT regards our employees as important assets and applies a structured process in relation to the employees' qualifications, training, and certifications. On an ongoing basis - and as a minimum annually - courses, presentations, and other relevant activities are organized to ensure that relevant employees and any relevant external partners are updated about security and made aware of any new threats.

All performing consultants have competencies within their areas of work. This is documented by means of relevant certifications and internal training.

Inventio.IT must meet a series of requirements from Microsoft, including specific requirements stating that a specified number of consultants have passed specified product certifications - certifications that must be renewed continuously. Inventio.IT ensures the maintenance of this high certification status via continual product training and course attendance.





## Physical and environmental security

Hardware related to ERP Online is placed at Interxion's data centres at different locations. The data centres have redundancy on all essential components of infrastructure, like power, UPS, emergency generators, networks as well as internet connection.

Interxion – the primary data centre – is placed in an enclosed area. The main entrance is always locked, and only employees with access card are able to unlock it.

Solely authorized persons get access to the premises via the established procedure, and at intervals – as a minimum once a year - we follow-up on the persons, who have this access. Only very few selected persons from Inventio.IT and MMT have access to Interxion.

The servers are placed in a locked room installed with cooling and firefighting equipment etc. The server room has central network equipment and is thus secured in the same way as the servers. Power supply for the operation of the data centre is protected by UPS and generator.

On an ongoing basis, control supervision is conducted in relation to IT security placed at Interxion (sub-contractor).

External persons (suppliers or customers) are only given access when accompanied by an authorized employee.

No unauthorized person will be able to walk around in Inventio.IT's offices unimpeded, as the exterior doors are locked and as a minimum require key card to unlock.

## User management / access security

At Inventio.IT there is an established policy for allocation of access. The policy is part of our IT security policy.

Customers' users are solely created based on our customers' requests, and likewise - auditor's access to end customers is only granted based on the end customer's acceptance.

Inventio.IT's own users are only created based on authorization in writing from the management. As a rule, users are created with the lowest set of rights necessary to carry out the assigned tasks. Inventio.IT's IT security policy prescribes that the employees' passwords are personal, and that only the user himself/herself is allowed to know the password.

- Password requirements – Password must consist of digits or letters
- Two-factor logon is applied.

To ensure the highest security level possible, only very few employees at Inventio.IT and MMT have been granted access to back-end systems in relation to ERP Online.

To grant access for a new user, approval from at least two persons from the ERP Online Department is required.

## Cryptography

Encryption is an important security measure used for protection of data during transportation and storing. Using secure encryption algorithms is decisive for maintenance of high security regarding data communication and storing. Usually, we use TLS (Transport Layer Security) version 1.2 or newer.

- Ensure network traffic between the user's client (browser) and Inventio.IT's services. HTTPS traffic is filtered through a firewall and redirected to central "load balancers."
- VPN (Virtual Private Network) tunnels are used to ensure the network traffic between customers, third parties, and Inventio.IT's network.
- SFTP (Secure File transport Protocol) is used for exchanging files between customers, third parties, and Inventio.IT.
- Secure mail, default setting is set up to use encryption for sending/receiving e-mail via SMTP.
- Backup of files and databases is performed locally and is secured using TLS 1.2 encryption.
- Storage disks (SAN) use encryption for disks that are actively registered in the SAN cluster. When a disk is removed, the encryption is automatically erased within short time.

### Development environment

When Inventio.IT develops apps, dedicated sandbox and test environments are used from where software is run for development and test. The said environments are different from the environments used for operations.

There are set procedures for development, test, and approval. Code changes are separated from the standard application.

### Change management

The purpose of change management is to ensure that changes are tested and tried out before the change is implemented for operation. All changes are logged automatically, and version control is used.

If incidents happen that might impact the operations, the monitoring system will automatically alert the emergency response organization, and there is an established procedure for escalation, ending with involving the CEO.

### Operating ERP Online Services

The operation of ERP Online is conducted by Inventio.IT in close collaboration with MMT.

### Monitoring

Automatic monitoring of servers, storage systems, networks etc. is established, and first line support staff is on duty 24/7/365. Inventio.IT supervises this control on an ongoing basis.

Furthermore, Inventio.IT monitors on application level to ensure optimal performance on the systems.

In case of a critical error, an alert is sent visually on a monitoring screen as well as on SMS. If a situation occurs, when an error is found on a component not included in the automatic monitoring, steps will be taken to future registration of this component in the system.


The hosting centre at Interxion is monitored in relation to power cut, temperature, fire, water, air humidity, and in addition the whole hosting centre has camera surveillance.

### Backup/ restore

The purpose of backup is to ensure that the customer's data at Inventio.IT A/S' ERP platform can be re-created, accurately and fast, in order to avoid unnecessary waiting time for the customers.

Inventio.IT ensures the re-establishing of systems and data in a suitable and correct matter and in accordance with the existing agreements with Inventio.IT's customers.

A test plan is established for verifying the integrity of the backup, as well as a test of how to re-establish systems and data in a practical way. A log of these tests is made, in order to follow-up on the possibilities of improving procedures and processes.



On a daily basis, backup is taken of the total ERP Online platform and the surrounding systems as well as of the customers' databases.

There are devised set procedures and descriptions for configuration and maintenance.

Every night a complete copy of all data from Inventio.IT's central systems is moved to the secondary data centre by means of the backup system. In this way, backup data is physically separated from the operational systems.

Tasks related to backup are carried out by both MMT and Inventio.IT. Inventio.IT monitors this control on an ongoing basis.

In the event, a customer wants a restore from backup or a readout of BAK file, such work is invoiced according to time spent.

### **Patch management**

The purpose of patch management is to ensure that all relevant updates such as patches, fixes and service packs from suppliers are implemented. This happens in order to protect the systems against downtime and unauthorized access. This also ensures that the implementation is made in a controlled manner.

All Windows servers are divided into different up-dating groups. Some servers are automatically updated immediately. Other servers are updated shortly hereafter, if the first update was successful. Critical servers are updated manually in order to increase the stability of operations.

There is devised a fall-back-plan in relation to patch management. The purpose of the fall-back-plan is ensuring that the systems can return to normal operations if the update does not work as intended.

Tasks regarding patch management are carried out by MMT in close dialogue with Inventio.IT, who also supervises this control on an ongoing basis.

### **Communications security**

The internet provider for the operations centre is Telia. There are two 2GB lines with separate routes to the data centre in Ballerup and two 1GB lines with separate routes to the data centre in Valby. In addition, there is a 6GB line between the 2 data centres, and both data centres are able to function as primary access to all systems.

There are redundant firewalls/routers in both data centres. Four of them at Ballerup and two of them at Valby. All firewalls are protected against DDOS by means of policies.


We are protected against ransomware using antivirus and spam filter.

Tasks related to communications security are carried out by MMT in close dialogue with Inventio.IT, who also supervises this control on an ongoing basis.

### **IT security incident management**

Security incidents detected via - our own observations, alerts from log and monitoring system, phone calls from customers/subcontractors/business partners, respectively - are forwarded to ERP Online with simultaneous information to the management of Inventio.IT.

Security incidents and weaknesses in Inventio.IT's systems must be reported in such a way that it is possible to carry out remedial action in a timely manner.



All employees at Inventio.IT are well aware of procedure reporting of various types of incidents and weaknesses that might have an impact on the security of Inventio.IT's operations. Security incidents and weaknesses must be reported to management as soon as possible.

It is the responsibility of management to define and coordinate a structured direction process to ensure an appropriate response to security incidents.

Tasks related to managing IT security incidents are carried out by MMT in close collaboration with Inventio.IT. Inventio.IT supervises this control on an ongoing basis.

### **Emergency response management**

Both Inventio.IT and MMT have devised a formal and set procedure for managing the contingency planning on all levels. The contingency plan includes IT systems and processes on all levels. The contingency plan is embedded in the IT risk analysis and is maintained – as a minimum once a year – in continuation of the completion of the analysis.

In devising and reviewing contingency plans, these plans are regularly assessed in relation to Inventio.IT's IT security policy in force.

Via membership of DCC (Danish Cloud Community) Inventio.IT is obliged to be able to re-establish any and all units in the data centre within three days. This is secured as risks have been balanced, units in operations have been classified, and procedures have been established ensuring that the contingency planning is able to replace the operations platform in order to re-establish the provided services in time.

A disaster recovery test of the emergency response is performed regularly. After completing the test, the result is analyzed, and on this background any relevant elements, procedures and plans are updated.

### **Compliance with the role as Data Processor**


It is the responsibility of Inventio.IT A/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
- Inventio.IT A/S Service Level Agreement
- Inventio.IT A/S standard contract or other relevant sources

Inventio.IT is obliged to involve legal experts as needed in order to ensure an appropriate level of compliance with law and regulations. Furthermore, management reviews all security policies on a regular basis, including involving any relevant stakeholders. The IT security framework is regularly audited by an independent, external party, and on request the audit report is shared with all Inventio.IT's customers.

#### *EU General Data Protection Regulation*

Inventio.IT's IT services support the customers' work processes in connection with ERP Online Services. Inventio.IT does not own any data the customers collect but develops and operates the IT services the customers utilize for performing the necessary processing of personal data. According to the EU General Data Protection Regulation and the Danish supplementary regulations (the Danish Data Protection Act), Inventio.IT A/S is the Data Processor, and the customer is the Data Controller.



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

According to GDPR, compliance with the ISO 27001+2 standard ensures an appropriate security level.

#### *Data Protection Officer (DPO)*

It is Inventio.IT's assessment, that a DPO is no mandatory requirement.

#### *Privacy and protection of personal data*

As mentioned above, Inventio.IT is the customers' Data Processor, given that the customers are offered an IT service to which they can transfer and handle data and use data for further processing within their respective IT tasks. Inventio.IT is not responsible for any data uploaded by the customers to their Inventio.IT It service. Based on the categories and confidence of data transferred for processing by the customer, Inventio.IT A/S must implement all necessary security measures needed in order to ensure an appropriate level of security.

Below is a description of Inventio.IT's procedures for operating as a Data Processor, following directions from the Data Controllers.

#### *Data Protection Agreements*


Inventio.IT enters Data Processor Agreements with all our customers. The Data Processor Agreement is a set procedure when entering a contract, and either Inventio.IT's own template is used or the customer's template. These contracts outline Inventio.IT's role and responsibilities as Data Processor.

As Data Processor Inventio.IT is subject to a special responsibility defined in the General Data Protection Regulation and implemented as requirements in a Data Processor Agreement. Inventio.IT must, inter alia:

- Keep record of the types of personal data processed in the respective IT services.
- Describe the technical and organisational security measures implemented in order to safeguard personal data.
- Contribute to the customer's obligations regarding the Data Subject's rights (see Chapter 3 in the EU General Data Protection Regulation - GDPR)
- Provide expertise for the customer in order to ensure compliance with Article 32 – 34 of GDPR:
  - Article 32 – Processing security
  - Article 33 – Reporting breaches of personal data security
  - Article 34 – Providing information about breaches of personal data security to the Data Subjects
- Comply with the customer's demands about transfer of any personal data outside of the EEA
- Register name and contact information of suppliers, who are sub-processors.
- Secure that requirements from the customer in relation to processing of personal data match the requirements to a sub-processor.

#### *Decision of purpose as well as legal basis*

As data processor, Inventio.IT works with personal data based on the customers' directions describing the restrictions regarding the limitations of the purpose for the use of data. In this way, it is the responsibility of Inventio.IT that data collected for a particular purpose is not processed contrary to the said purpose.



The legal basis for processing personal data in relation to the IT operation of ERP Online provided by Inventio.IT is found in the data controller's compliance with legal obligations or in performance of obligations under a contract.

#### *Access to data in customer instances*

Inventio.IT offers ERP Online Services operated by Inventio.IT's operations department. In general, Inventio.IT has no access to any customer instances unless specific tasks speak in favour of doing so.

Inventio.IT has laid down principles for employees' access to and processing customers' data.

- Only trusted employees have access to customer data and only when there is a work-related need.
- Comprehensive introduction courses focusing on rules regarding processing customer data, as well as follow-up in the form of awareness campaigns.
- Procedure for granting, review, and control of access to customer data.
- Rules for processing customer data in Inventio.IT's ISMS.

Inventio.IT logs and monitors access to the customers' data in order to secure that no unauthorized persons get access, and that no granted access is violated.

### **Important changes in relation to IT security**

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

### **Customers' responsibilities (complementary controls at the customer)**

This Chapter describes the general control environment for Inventio.IT's ERP Online Services, which means that no account has been made for the agreements of individual customers.

Inventio.IT is not responsible for access right, including granting, changing, and removal, in relation to the individual customer's users and their access to Inventio.IT's ERP Online Services. The customer is responsible for ensuring any controls necessary in connection with this control objective. In relation to management of the password security, the audit is performed from a general point of view.

For some user companies the security in relation to creation of passwords might be below the frame if the customer's management wanted it. The responsibility for reconciliation of the control environment for password security stays with each user company, and with those using this report.

Customers are responsible for data transmission to Inventio.IT's ERP Online Services, and it is the customers' responsibility to create the necessary data transmission to Inventio.IT's data centre. The customer must ensure the necessary control measures in relation to this control objective.

Inventio.IT's continuity management is constructed based on an overall contingency plan that describes the approach and procedures to be applied if recovery of Inventio.IT A/S' ERP Online Services is needed. Specific contingency plans can be prepared for the individual customer according to need in proportion to the risk of interrupting business processes.

## APPENDIX 1:

# Inventio.IT A/ S applies the following control objectives and security measures from ISO27001 and 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
  - 6.2. Mobile devices and teleworking
- 

### 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
- 

### 9. Access control

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

### 10. Cryptography

- 10.1. Cryptographic controls
- 

### 12. Operations security

- 12.1. Operational procedures and responsibilities
- 12.2. Protection from malware
- 12.3. Backup
- 12.4. Logging and monitoring
- 12.5. Operational software management

### 13. Communications security

- 13.1. Network security management
- 

### 14. (Acquisition), development, and maintenance of systems

- 14.1. Security requirements to the IT system
  - 14.2. Security in development and assisting processes
- 

### 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

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

For the customers of Inventio.IT A/S' ERP Online Services and their auditors

## Scope

We have been engaged to report on Inventio.IT A/S' description in Chapter 2 (incl. Appendix 1), which is a description of the control environment in connection with the IT operations of ERP Online Services, see Data Processor Agreements with customers, throughout the period 1 January 2024 - 31 December 2024, 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 that the present report does not include the IT security controls and control activities related to the use of external business partners. The report does not include control or supervision of subcontractors. These subcontractors are listed in the 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 under the section: Complementary controls at the customer.

## Inventio.IT A/ S' responsibility

Inventio.IT A/S is responsible for the preparation of the description in Chapter 2 and accompanying assertion in Chapter 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 ISQM 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 Inventio.IT A/S'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 whe-





ther, 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 Inventio.IT 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 Inventio.IT A/ S**

Inventio.IT A/S'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 Inventio.IT 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 Inventio.IT A/S' control environment in relation to the IT operations of ERP Online Services, such as it was designed and implemented throughout the period 1 January 2024 - 31 December 2024 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 January 2024 - 31 December 2024; 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 January 2024 - 31 December 2024.

### **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 Inventio.IT 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 as Data Controllers have performed themselves, when assessing whether the control environment is appropriate, and there is compliance with the requirements of General Data Protection Regulation.



Søborg, 9 January 2025

**Beierholm**

Godkendt Revisionspartnerselskab  
CVR-nr. 32 89 54 68

**Kim Larsen**

State-authorized Public Accountant

**Jesper Aaskov Pedersen**

IT-auditor, Director

## 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 Inventio.IT A/S has complied with the control objectives throughout the period 1 January 2024 - 31 December 2024.

Below the grey field are three columns:

- The first column tells the activities Inventio.IT A/S, according to their 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 assess, 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 Inventio.IT 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.

## Risk Assessment and Management

The risk assessment must identify and prioritise the risks based on the operation of ERP Online Services. The findings are to contribute to the identification and prioritisation of management interventions and security measures necessary to address relevant risks.

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
<p>Through a risk assessment, risks have been identified and prioritised. The ERP Online Services defined in the description are used as basis for the assessment.</p> <p>The findings contribute to the identification and prioritisation of management interventions and security measures necessary to address relevant risks.</p>	<p>We have requested and obtained the relevant material in connection with the audit of risk management.</p> <p>We have checked that regular risk assessments are carried out for the ERP Online Services in relation to business conditions and their development. We have checked that the risk assessment is deployed down through the company's organisation.</p> <p>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.</p>	<p>No comments.</p>

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 is maintained, taking the current risk assessment into consideration.

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
<p>There is a written strategy covering, among other things, Management's security objectives, policies, and overall action plan.</p> <p>The IT security policy and accompanying supporting policies are approved by the company's Management, and then deployed down through the company's organisation.</p> <p>The policy is available for all relevant employees.</p> <p>The policy is re-evaluated according to planned intervals.</p>	<p>We have obtained and audited Inventio.IT A/S' latest IT security policy.</p> <p>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.</p> <p>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 Inventio.IT A/S' intranet.</p>	<p>No comments.</p>

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.

Management must ensure a suitable level of protection for teleworking and the use of mobile devices.

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
<p>Organisational responsibility for IT security has been placed, documented, and implemented.</p> <p>The IT security has been coordinated across the company's organisation.</p>	<p>Through inspection and tests, we have ensured that the organisational responsibility for IT security is documented and implemented.</p> <p>We have checked that the IT security is deployed across the organisation in relation to ERP Online Services.</p> <p>By conducting interviews, we have checked that the person responsible for IT security knows his/her role and responsibilities.</p>	No comments.
<p>Risks in relation to use of mobile devices and teleworking have been identified, and security issues in relation customers are managed.</p>	<p>We checked that formal policies exist in connection with the use of mobile devices and teleworking.</p> <p>On a test basis, we have inspected that the policy is implemented regarding employees using mobile devices.</p> <p>Regarding the use of teleworking at Inventio.IT A/S, we have checked whether appropriate security measures have been implemented thus this area is covered in relation to the risk assessment of the area.</p>	No comments.

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.

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
<p>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 Inventio.IT A/S. This includes the framework laid down for the work and the IT security involved.</p> <p>Security responsibilities, if any, are determined and described in job descriptions and in the form of terms and conditions in the employment contract.</p> <p>The employees are familiar with their professional secrecy based on a signed employment contract and through Inventio.IT A/S' HR policy.</p>	<p>We have verified that routines and procedures developed by Management in connection with start of employment and termination of employment have been adhered to.</p> <p>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.</p> <p>Through interviews, we have checked that employees of significance to ERP Online Services are familiar with their professional secrecy.</p> <p>We have on a test basis 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.</p> <p>We have ensured that Inventio.IT 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 Inventio.IT A/S.</p>	<p>No comments.</p>

Penneo dokumentnøgle: 1027Z-SPJSU-JJEAG-5YOAA-LE8FW-FVX6X

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 indentified, and a responsible owner appointed. The company must ensure that information assets related to ERP Online Services have an appropriate level of protection.

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
<p>All information assets have been identified and an updated list of all significant assets has been established.</p> <p>An "owner" of all significant assets is appointed in connection with the operation of ERP Online Services.</p>	<p>We have examined and checked the company's central IT register for significant IT entities in connection with the operation of Inventio.IT A/S' ERP Online Services.</p> <p>Through observations and control, we checked relations to central knowhow systems for the operation of ERP Online Services.</p> <p>By observations and enquiries, we have checked that Inventio.IT A/S complies with all material security measures for the area in accordance with the security standard.</p>	<p>No comments.</p>



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 secured, and unauthorised access must be prevented.

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
Documentation and updated directions exist for Inventio.IT A/S' access control.	<p>We have:</p> <ul style="list-style-type: none"> <li>asked Management, whether access control procedures have been established at Inventio.IT A/S.</li> <li>verified on a test basis that access control procedures exist and have been implemented; see Inventio.IT A/S' directions.</li> <li>by interviewing key staff and by inspection on a test basis, we have verified that access control for the operations environment comply with Inventio.IT A/S' directions, and authorisations are granted according to agreement.</li> </ul>	No comments.
<p>A formal procedure exists for granting and discontinuing user access.</p> <p>Granting and application of extended access rights are limited and monitored.</p>	<p>We have asked Management, whether a formal procedure exists for granting and discontinuing user access.</p> <p>We have by inspection on a test basis verified:</p> <ul style="list-style-type: none"> <li>that adequate authorisation systems are used in relation to access control at Inventio.IT A/S.</li> <li>that the formalised business procedures for granting and discontinuing user access have been implemented in Inventio.IT A/S' systems, and registered users are subject to regular follow-up.</li> </ul>	No comments.
Internal users' access rights are reviewed regularly according to a formalised business procedure.	<p>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:</p> <ul style="list-style-type: none"> <li>that formal management follow-up is performed on registered users with ordinary rights and extended rights every 12 months.</li> </ul>	No comments.

<p>The granting of access codes is controlled through a formalised and controlled process, which ensures, among other things, that standard passwords are changed.</p>	<p>We have asked Management whether procedures granting access code have been established at Inventio.IT A/S.</p> <p>By inspection on a test basis, we have verified</p> <ul style="list-style-type: none"> <li>• that an automatic systems control takes place, when access codes are granted to check that passwords are changed after first login.</li> <li>• that standard passwords are changed in connection with implementation of systems software, etc.</li> <li>• if this is not possible, that procedures ensure that standard passwords are changed manually.</li> </ul>	<p>No comments.</p>
<p>Access to operating systems and networks are protected by passwords.</p> <p>Quality requirements have been specified for passwords, which must have a minimum length, requirements as to complexity, maximum duration, and likewise password setup means that passwords cannot be reused. In addition, 2-factor logon is a requirement.</p> <p>Furthermore, the user will be barred, in the event of repeated unsuccessful attempts to login.</p>	<p>We have asked Management whether procedures ensuring quality passwords in Inventio.IT A/S are established.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• minimum length of password</li> <li>• maximum life of password</li> <li>• minimum history of password</li> <li>• lockout after unsuccessful login attempts</li> <li>• 2-factor logon</li> </ul>	<p>No comments.</p>

CONTROL OBJECTIVE 10:

## Cryptography

There must be correct and efficient use of cryptography to protect information confidentiality, authenticity, and/or integrity.

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
<p>For encrypting personal data Inventio.IT A/S has implemented an encrypting policy defining the strength and protocol of encrypting.</p> <p>Encryption is used when transmitting confidential and sensitive personal data via internet and e-mail.</p>	<p>Inspected the existence of formalized procedures ensuring that transmission of sensitive and confidential information via the internet is protected by strong encryption based on an approved algorithm.</p> <p>Inspected that encryption is applied when sensitive and confidential personal data is transmitted via internet or using e-mail.</p> <p>Inspected that technological solutions for encryption have been accessible and activated throughout the entire reporting period.</p>	<p>No comments.</p>

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.

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
<p>The operations procedures for business-critical systems are documented, and they are available to staff with work-related needs.</p> <p>Management has implemented policies and procedures to ensure satisfactory segregation of duties.</p>	<p>We have:</p> <ul style="list-style-type: none"> <li>• Asked Management whether all relevant operation procedures are documented.</li> <li>• 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.</li> <li>• 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.</li> </ul>	<p>No comments.</p>
<p>Management of operational environment is established in order to minimise the risk of technology related crashes.</p> <p>Continuous capacity projection is performed based on business expectations for growth and new activities and the capacity demands derived hereof.</p>	<p>We have:</p> <p>Asked Management about the procedures and control activities performed.</p> <p>On a test basis examined that the operation environment's consumption of resources is monitored and adapted to the expected and necessary capacity requirements.</p>	<p>No comments.</p>

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.

Inventio.IT A/S' control procedures	Auditor's test of control procedures	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.	<p>We have:</p> <ul style="list-style-type: none"> <li>enquired about and inspected the procedures/ control activities performed in the event of virus attacks or outbreaks.</li> <li>enquired about and inspected the activities meant to increase the employees' awareness of precautions against virus attacks or outbreaks.</li> <li>verified that anti-virus software has been installed on servers and inspected signature files documenting that they are updated.</li> </ul>	No comments.

Control objective: Backup

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

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
Backup is made of all the company's significant information assets, including, e.g. parameter setup and other operations-critical documentation, according to the specified directions.	<p>We have:</p> <ul style="list-style-type: none"> <li>asked Management about the procedures/ control activities performed.</li> <li>examined backup procedures on a test basis to confirm that these are formally documented.</li> <li>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.</li> <li>examined physical security (e.g. access limitations) for internal storage locations to confirm that backup is safely stored.</li> </ul>	No comments.

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.

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
<p>Operating systems and network transactions or activities involving special risks are monitored. Abnormal conditions are examined and resolved on a timely basis.</p> <p>Inventio.IT A/S logs when internal users log off and on the systems.</p> <p>Only in the event of suspected or identified abuse of the systems, users are actively monitored.</p>	<p>We have:</p> <ul style="list-style-type: none"> <li>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.</li> <li>checked on a test basis that logs from critical systems are subject to sufficient follow-up.</li> </ul>	<p>No comments.</p>
<p>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.</p> <p>Alerts are shown on the monitoring screen mounted in the project and operations department. Critical alerts are also sent by email and SMS.</p> <p>Status reports are sent by email from different systems. Some daily – others when incidents occur in the system. The operator on duty is responsible for checking these emails daily.</p>	<p>We have:</p> <ul style="list-style-type: none"> <li>asked Management about the procedures/ control activities performed.</li> <li>ensured that a monitoring tool is used and that this is available to all employees.</li> <li>ensured that alerts are sent by email and SMS, if errors occur.</li> <li>examined status reports.</li> <li>ensured that an operator on duty is established and that this operator on duty checks reports on a daily basis.</li> </ul>	<p>No comments.</p>

Control objective: Managing operations software

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

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
<p>Changes in the operation environment comply with established procedures.</p>	<p>We have asked Management, whether procedures for patch management are established in Inventio.IT A/S.</p> <p>By inspection on test basis, we have verified that</p> <ul style="list-style-type: none"> <li>• adequate procedures are applied, when controlled implementation of changes to the production environment of Inventio.IT A/S is performed.</li> <li>• changes to Inventio.IT A/S' operation environment comply with directions in force, including correct registration and documentation of applications about changes.</li> </ul> <p>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.</p>	<p>No comments.</p>
<p>Changes in existing user systems and operation environments comply with formalised procedures and processes.</p>	<p>We have asked Management, whether procedures for patch management are established in Inventio.IT A/S.</p> <p>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</p> <ul style="list-style-type: none"> <li>• applications for change are registered and described.</li> <li>• all changes are subject to formal impact assessments before implementation.</li> <li>• All changes are subject to formal impact assessments</li> <li>• fall-back plans are described</li> <li>• systems affected by changes are identified.</li> <li>• Documented test of changes is performed before they are put into operation</li> <li>• documentation is updated reflecting the implemented changes in all material respects.</li> <li>• procedures are subject to managing &amp; coordination by a "Change Board"</li> </ul>	<p>No comments.</p>

Penneo dokumentnøgle: 1027Z-SPJSU-JJEAG-5YOAA-LE8FW-FVX6X

CONTROL OBJECTIVE 13:

## Communications Security

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

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
<p>Networks must be protected against threats in order to secure network-based systems and the transmitted data.</p> <p>Production environment must be secured against failing supply in relation to redundancy to network connection to the internet.</p> <p>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.</p>	<p>It has been checked that necessary protection against unauthorised access is implemented, including:</p> <ul style="list-style-type: none"> <li>• Appropriate procedures for managing network equipment are established.</li> <li>• Segregation of user functions is established.</li> <li>• Appropriate logging and monitoring procedures as well as follow-up are established.</li> <li>• Managing the company's network is coordinated in order to ensure optimal utilisation and a coherent security level.</li> <li>• Ensured that connections for data communication with the internet are established via more than one ISP supplier.</li> <li>• 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.</li> </ul>	<p>No comments.</p>
<p>Adequate procedures for managing threats in the form of attacks from the internet (cyber-attacks) must be implemented.</p> <p>In this connection, tools for managing the contingency approach in the event of a cyber-attack must be devised.</p>	<p>We have controlled that an adequate number of procedures with accompanying contingency plans regarding managing threats in relation to cyber-attacks are implemented.</p> <p>By inspection on a test basis, we have ensured:</p> <ul style="list-style-type: none"> <li>• that appropriate framework for managing cyber-attacks is devised.</li> <li>• that plans for managing the threat are devised and implemented.</li> <li>• that the plans include cross-organisational collaboration between internal groups.</li> </ul>	<p>No comments.</p>



CONTROL OBJECTIVE 14:

## (Acquisition), development and maintenance of systems

Ensure that ERP Online Services are managed with adequate IT-security, including an appropriate segregation of functions between production environment and development environment.

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
<p>Inventio.IT A/S has prepared system development and maintenance activities based on a proprietary project model.</p> <p>The development organisation is structured with a central steering committee having the responsibility for creating suitable procedures and accompanying management controls.</p> <p>All changes to be implemented in the production environment must be approved by the development group responsible for the ERP Online Service solution in question.</p> <p>Software development must be placed in independent test environments.</p>	<p>We have:</p> <ul style="list-style-type: none"> <li>asked management whether a general quality management model has been prepared for the handling of software development</li> <li>In connection with the audit, controlled the existence of procedures and routines for roll-out of software changes</li> </ul> <p>The user management secures an appropriate control in relation to handling the logical access control.</p> <p>On a sample basis, we have controlled that all user activities are registered and logged in a central database. The IT Security Manager reviews the logging database on a regular basis.</p> <p>We have controlled the existence of procedures for segregation between the production environment and the environment for development and maintenance.</p> <p>In connection with our audit, we have checked the existence of segregated test environments for the software development.</p> <p>On a sample basis we have tested that the production environment for software development takes place from an independent IP segment.</p>	<p>No comments.</p>

CONTROL OBJECTIVE 15:

## Supplier Relationships

External business partners are obliged to comply with the company's established framework for IT security level.

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
Risks related to external business partners are identified, and security in third-party agreements are managed.	<p>We have verified that in connection with the use of external business partners there are formal cooperation agreements.</p> <p>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.</p>	No comments.
In case of changes with impact on the production environment, and where services from external suppliers are used, suppliers are selected through collaboration between the Operations Manager and the IT Security Manager. Solely approved suppliers are used.	<p>We have asked Management about relevant procedures applied in connection with selecting external partners.</p> <p>We have ensured that appropriate procedures for managing cooperation with external partners are established.</p> <p>We have tested that key suppliers have updated and approved contracts.</p>	No comments.
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.	No comments.

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.

Inventio.IT 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.	<p>We have asked Management whether procedures are established for reporting security incidents.</p> <p>We have verified that procedures and routines are devised for reporting and handling of security incidents, and that the reporting is submitted to the right places in the organisation; see Directions.</p> <p>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.</p>	No comments.

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.

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
<p>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.</p>	<p>We have asked Management whether business continuity management has been devised for ERP Online Services at Inventio.IT A/S.</p> <p>By inspection on a test basis, we have verified</p> <ul style="list-style-type: none"> <li>• that appropriate framework for preparation of business continuity management has been established</li> <li>• that contingency plans are prepared and implemented</li> <li>• that the plans include business continuity management across the organisation</li> <li>• that the plans include appropriate strategy and procedures for communication with the stakeholders of Inventio.IT A/S.</li> <li>• that contingency plans are tested on a regular basis</li> <li>• that maintenance and reassessment of the total basis for business continuity management is undertaken on a regular basis.</li> </ul>	<p>No comments.</p>

CONTROL OBJECTIVE 18:

## Compliance with the Role as Data Processor

**Principles for processing personal data:**

There is compliance with procedures and controls ensuring that collecting, processing, and storing of personal data are performed in accordance with the agreements for processing personal data.

Inventio.IT 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.	No comments.
Only the kind of processing of personal data included in directions from Data Controller is performed.	We have controlled that Management ensures that processing of personal data is solely performed in accordance with directions.  We have checked, using a sample consisting of a suitable number of processing that processing is performed according to directions.	No comments.
Management immediately informs the Data Controller, if Directions in the Data Processor's view is contrary to the General Data Protection Regulation or data protection provisions according to other EU legislation or the national legislation of the member states.	We have controlled that Management ensures that processing is reviewed and the existence of formalised procedures securing that processing of personal data is not performed against the EU General Data Protection Regulation or other legislation.  We have controlled the existence of procedures for informing the Data Controller in cases when processing of personal data is deemed to be against legislation.  We have controlled that the Data Controller was informed in cases when processing of personal data was deemed to be against legislation.	No comments.

### Data Processing:

There is compliance with procedures and controls ensuring that personal data can be erased or returned if an agreement is entered with the Data Controller.

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
<p>There are procedures in writing with requirements about storing and erasing of personal data in accordance with the agreement with the Data Controller.</p> <p>On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.</p>	<p>We have controlled that there are formalised procedures for storing and erasing of personal data in accordance with the agreement with the Data Controller.</p> <p>We have checked that the procedures are updated.</p>	No comments.
<p>According to the agreement with the Data Controller, when processing of personal data is finished, data are</p> <ul style="list-style-type: none"><li>• Returned to the Data Controller, and/or</li><li>• Erased, when erasing is not against other legislation.</li></ul>	<p>We have controlled that there are formalised procedures for handling the Data Controllers' data when processing of personal data is finished.</p> <p>We have controlled by random check using a suitable population of finished data processing cases that conducting the agreed erasing or returning of data is documented.</p>	No comments.
<p>There are procedures in writing including demands that personal data is only stored in accordance with the agreement with the Data Controller.</p> <p>On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.</p>	<p>We have controlled that there are formalised procedures ensuring that storing and processing of personal data are solely undertaken according to the Data Processor Agreements.</p> <p>We have checked that the procedures are updated.</p> <p>We have controlled on sample basis, whether documentation exists that data processing is conducted in accordance with the Data Processor Agreement.</p>	No comments.

**The Data Processor's responsibility:**

There is compliance with procedures and controls ensuring that solely 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.

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
<p>There are procedures in writing including demands to the Data Processor in relation to use of sub-processors, including demands about Sub-processor Agreements and Directions.</p> <p>On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.</p>	<p>We have controlled that there are formalised procedures regarding the use of sub-processors, including demands about Sub-processor Agreements and Directions.</p> <p>Inspected that procedures are updated.</p>	<p>No comments.</p>
<p>For processing personal data, the Data Processor solely uses Sub-processors, who are specifically or generally approved by the Data Controller.</p>	<p>Inspected that the Data Processor has a complete and updated list of the sub-processors used. Inspected using a sample of 4 Sub-processor from the Data Processor's list that it is documented that the Sub-processor's data processing is included in the Data Processor Agreements – or in other ways approved by the Data Collector.</p>	<p>No comments.</p>
<p>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 must be approved by the Data Controller.</p>	<p>We have controlled that formalized procedures are in place for informing the Data Controller when changing the sub-processors used.</p> <p>Inspected documentation that the Data Controller was informed when changing the sub-processors used throughout the assurance period.</p>	<p>No comments.</p>
<p>The Data Processor has placed the same data protection obligations on the sub-processors as the obligations included in the Data Processor Agreement or similar document with the Data Controller.</p>	<p>We have controlled the existence of signed Sub-processor Agreements with all sub-processors used and included in the Data Processor's list.</p> <p>Inspected using a sample of 4 Sub-processor Agreement that the agreements include the same demands and obligations as stated in the Data Processor Agreements between the Data Controllers and the Data Processor.</p>	<p>No comments.</p>

<p>The Data Processor has a list of approved sub-processors including the following information:</p> <ul style="list-style-type: none"> <li>• Name</li> <li>• CVR.no.</li> <li>• Address</li> <li>• Outline of the processing</li> </ul>	<p>We have controlled that the Data Processor has a total and updated list of approved sub-processors used.</p> <p>Inspected that the list as a minimum includes the required information about each sub-processor.</p>	<p>No comments.</p>
--	---	---------------------

**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 processing of personal data as well as providing information about the processing of personal data to the Data Subjects.

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
<p>Written procedures exist which include a requirement that the Data Processor must assist the Data Controller in relation to the rights of Data Subjects.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>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.</p> <p>Inspected that procedures are up to date.</p>	<p>No comments.</p>
<p>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 processing as well as providing information about the processing of personal data to Data Subjects.</p>	<p>We have controlled that the procedures in place for assisting the Data Controller include detailed procedures for:</p> <ul style="list-style-type: none"> <li>• Handing out data;</li> <li>• Correcting data;</li> <li>• Deleting data;</li> <li>• Restricting the processing of personal data;</li> <li>• Providing information about the processing of personal data to Data Subjects.</li> </ul> <p>Inspected documentation that the systems and databases used support the performance of the said relevant detailed procedures.</p>	<p>No comments.</p>



#### Records of processing activities:

There is compliance with procedures and controls ensuring that the Data Processor keeps records of processing personal data for which the Data Processor is responsible.

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
There are records of the processing activities for each activity in ERP Online Services in combination with the relevant Data Controller.	We have controlled documentation displaying the existence of records for processing activities for each activity in ERP Online Services combined with the relevant Data Controller.	No comments.
Assessment is made on an ongoing basis – and at least once a year – that 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.	No comments.

#### Reporting breaches of personal data security to the Supervisory Authority (the Danish Data Protection Agency):

There is compliance with procedures and controls ensuring that any security breaches are managed in accordance with the entered Data Processor Agreement.

Inventio.IT A/S' control procedures	Auditor's test of controls	Test findings
There are procedures in writing - updated at least once a year – describing how to manage personal data security breaches including timely communication to the Data Controller.	We have controlled the existence of updated procedures in writing regarding managing personal data security breaches, including description of timely communication to the Data Controller.	No comments.
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.	No comments.
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.	No comments.