



# itm8 A/S

**Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 January 2025 to 31 December 2025 pursuant to the data processing agreement with data controllers**

**February 2026**



## Contents

1. Management's assertion .....	3
2. Independent auditor's report .....	5
3. Description of personal data processing .....	8
4. Control objectives, control activity, tests and test results .....	15

# 1. Management's assertion

itm8 A/S (itm8) processes personal data on behalf of data controllers in accordance with data processing agreements.

The accompanying description has been prepared for data controllers who have used services provided by itm8 | Managed Services and who have a sufficient understanding to consider the description along with other information, including information about controls operated by the data controller itself in assessing whether the requirements of the EU regulation on the "Protection of natural persons with regard to the processing of personal data and on the free movement of such data" and "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (subsequently "the data protection rules") have been complied with.

B4Restore and Keepit are subprocessors that provide backup services to itm8. This report uses the carve-out method, and the description in section 3 includes only the control objectives and related controls of itm8 and excludes the control objectives and related controls of B4Restore and Keepit. Our evaluation did not extend to controls of B4Restore and Keepit.

The description indicates that certain control objectives specified in the description can be achieved only if the complementary controls at the data controllers contemplated in the design of our controls are suitably designed and operating effectively. This report does not comprise the suitability of the design or operating effectiveness of such complementary controls at the data controllers.

itm8 confirms that:

- a) The accompanying description in section 3 fairly presents information security and measures in relation to the services provided by itm8 | Managed Services that have processed personal data for data controllers subject to the data protection rules throughout the period from 1 January 2025 to 31 December 2025. The criteria used in making this statement were that the accompanying description:
  - (i) Presents how information security and measures in relation to the services provided by itm8 | Managed Services were designed and implemented, including:
    - The types of services provided, including the type of personal data processed
    - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete and restrict processing of personal data
    - The procedures used to ensure that data processing has taken place in accordance with contract, instructions or agreement with the data controller
    - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality
    - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation
    - The procedures supporting, in the event of breach of personal data security, that the data controller may report this to the supervisory authority and inform the data subjects
    - The procedures ensuring appropriate technical and organisational security measures in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

- Controls that we, in reference to the scope of the services provided by itm8 | Managed Services, have assumed would be implemented by the data controllers and which, if necessary in order to achieve the control objectives stated in the description, are identified in the description
  - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data
- (ii) Includes relevant details of changes to the services provided by itm8 | Managed Services for processing personal data in the period from 1 January 2025 to 31 December 2025
- (iii) Does not omit or distort information relevant to the scope of the services provided by itm8 | Managed Services being described for the processing of personal data, while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the services provided by itm8 | Managed Services that each individual data controller may consider important in its own particular circumstances.
- b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 January 2025 to 31 December 2025. The criteria used in making this statement were that:
- (i) The risks that threatened achievement of the control objectives stated in the description were identified
  - (ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved
  - (iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 January 2025 to 31 December 2025.
- c) Appropriate technical and organisational measures were established and maintained to comply with the agreements with the data controllers, sound data processing practices and relevant requirements for data processors in accordance with the data protection rules.

Herning, 17. February 2026  
**itm8 A/S**

Frank Bech Jensen  
Head of Compliance and Security

## 2. Independent auditor's report

### Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 January 2025 to 31 December 2025 pursuant to the data processing agreement with data controllers

To: itm8 A/S (itm8) and data controllers

#### Scope

We have been engaged to report on itm8's description in section 3 of the services provided by itm8 | Managed Services in accordance with the data processing agreement with data controllers throughout the period from 1 January 2025 to 31 December 2025 (the description) and on the suitability of the design and operating effectiveness of controls related to the control objectives stated in the description.

Our report covers whether itm8 has designed and effectively operated suitable controls related to the control objectives stated in section 4. The report does not include an assessment of itm8's general compliance with the requirements of the EU regulation on the "Protection of natural persons with regard to the processing of personal data and on the free movement of such data" and "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (subsequently "the data protection rules").

B4Restore and Keepit are subprocessors that provide backup services to itm8. This report uses the carve-out method, and the description in section 3 includes only the controls objectives and related controls of itm8 and excludes the control objectives and related controls of B4Restore and Keepit. Our examination did not extend to controls of B4Restore and Keepit.

The description indicates that certain control objectives specified in the description can be achieved only if the complementary controls at the data controllers contemplated in the design of itm8's controls are suitably designed and operating effectively. This report does not comprise the suitability of the design or operating effectiveness of such complementary controls at the data controllers.

We express reasonable assurance in our conclusion.

#### itm8's responsibilities

itm8 is responsible for: preparing the description and accompanying assertion in section 1, including the completeness, accuracy and method of presentation of the description and assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; identifying the criteria and designing, implementing and effectively operating controls to achieve the stated control objectives. The control objectives have been specified by itm8 and are stated in the description.

#### Auditor's independence and quality control

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

Our firm applies International Standard on Quality Management 1, ISQM 1, which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

#### Auditor's responsibilities

Our responsibility is to express an opinion on the fairness of itm8's description and on the suitability of the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures.

We conducted our engagement in accordance with ISAE 3000 (revised), “Assurance engagements other than audits or reviews of historical financial information”, and additional requirements applicable in Denmark to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description of a data processor’s system and on the suitability of the design and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the description and the design and operating effectiveness of controls. The procedures selected depend on the data processor’s auditor’s judgement, including the assessment of risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. 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 by the data processor and described in section 1.

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

### **Inherent limitations**

itm8’s description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the services provided by itm8 | Managed Services that the individual data controller may consider important in its own particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect all personal data breaches. Also, the projection to future periods of any evaluation of the fairness of the presentation of the description, or opinions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a data processor may become inadequate or fail.

### **Opinion**

In our opinion, in all material respects, based on the criteria including the control objectives described in itm8’s assertion in section 1:

- a) The description fairly presents information security and measures in relation to the services provided by itm8 | Managed Services as designed and implemented throughout the period from 1 January 2025 to 31 December 2025
- b) The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls operated effectively throughout the period from 1 January 2025 to 31 December 2025, and if the data controllers applied the complementary controls referred to in section 3
- c) The controls tested, which together with the complementary controls at the data controllers referred to in section 3, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 January 2025 to 31 December 2025.

### **Description of test of controls**

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



## Intended users and purpose

We were engaged to report by itm8 and, therefore, this report and the description of tests of controls and results thereof in section 4 are intended for the use of itm8.

We permit the disclosure of this report in full only, including the description of tests of controls and results thereof by itm8, at its discretion, to the data controllers who have used the services provided by itm8 | Managed Services during some or all of the period from 1 January 2025 to 31 December 2025, who have a sufficient understanding to consider it, along with other information about controls operated by the data controllers themselves, without assuming or accepting any responsibility or liability to the data controllers on our part.

Our report is not to be used for any other purpose or to be distributed to any other parties.

Aarhus, 17. February 2026

**PricewaterhouseCoopers**

Statsautoriseret Revisionspartnerselskab

CVR no. 33 77 12 31

Jesper Parsberg Madsen  
State-Authorised Public Accountant  
mne26801

Iraj Bastar  
Director

### 3. Description of personal data processing

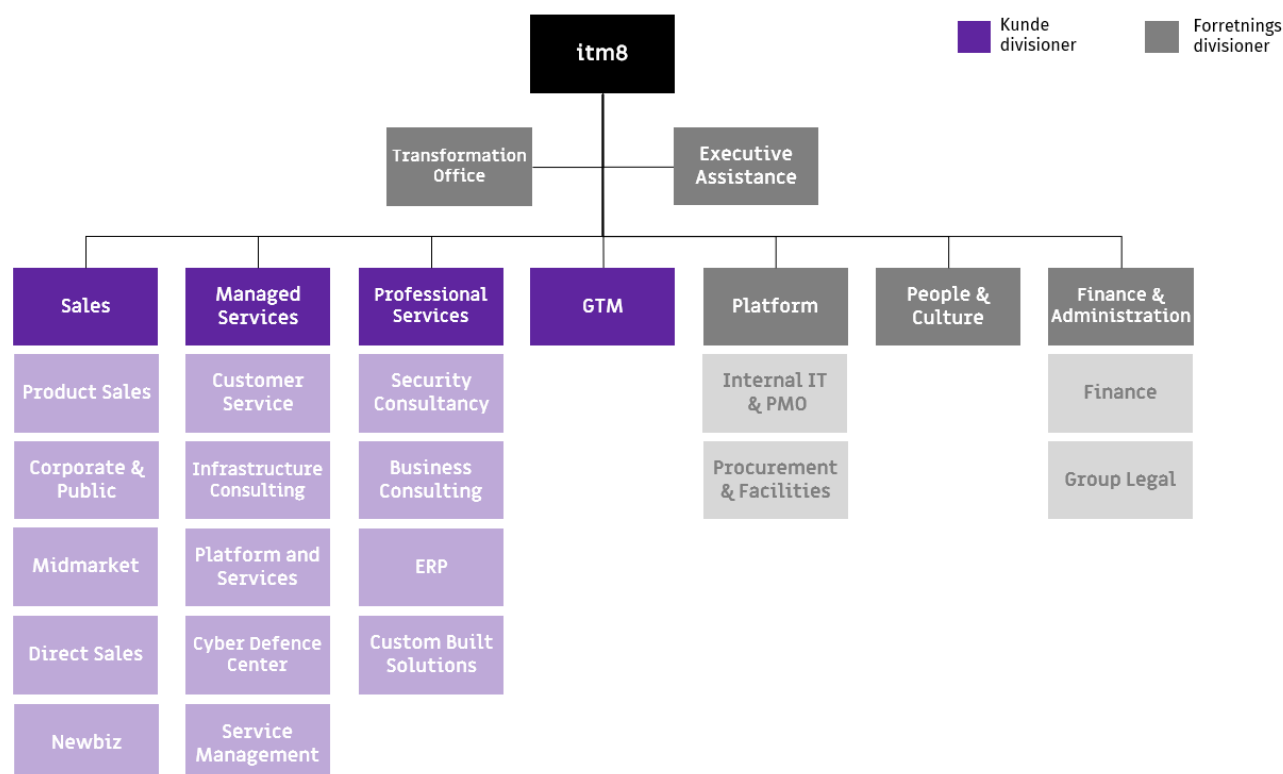
The purpose of the data processor's activities in connection with the processing of personal data on behalf of the data controller is to provide the agreed services described in the contracts between the data controller and the data processor. These services include hosting and operations, support, database administration, configuration and development, security services, application services and consulting services.

The instructions for data processing provided by the data controller are clearly defined in the data processing agreement between the respective parties. This framework ensures that the processing activities are in line with the contractual obligations and regulatory requirements.

#### 3.1. Description of the service organisation

itm8 A/S has undergone a significant development and has become a more structured organisation that provides managed IT services and professional services. Itm8 A/S Denmark is established based on twelve independent IT companies, all of which are owned by the itm8 Group. All twelve companies have now been legally and organisationally merged into itm8 A/S, which in addition to the Danish locations also includes itm8's global delivery locations in the Czech Republic and the Philippines. As a natural part of the merger, a major transition is now taking place to consolidate and unify services, processes and systems.

All companies have been merged into itm8 A/S's customer-oriented departments that drive service deliveries, while business divisions ensure necessary administrative and operational support. This structure enables itm8 to provide integrated and reliable services that meet high requirements in information security, quality and compliance to a wide range of customers.



Scope of itm8 ISAE-3000 independent assurance report

This independent audit report focuses on services provided by itm8's customer divisions, Managed Services and Professional Services, where personal data is processed as part of the provision of the service.

The report also includes itm8 A/S's global supply organisation, which in addition to Denmark includes itm8 Czech Republic and itm8 Philippines.

## Customer divisions

The customer-oriented divisions constitute itm8's primary service areas, with each division dedicated to specific areas of expertise:

- **Managed Services**

With a focus on cloud solutions and IT infrastructure, this division helps customers implement robust hosting and operational strategies. The division translates customers' business strategies into scalable cloud and infrastructure solutions through platform evaluations, security policy design, migrations, modernisation and 24/7 support.

Managed Services provides services to customers within support, operations, application operations, database administration and consulting services. Managed Services also includes the Cyber Defense Center, a division that offers comprehensive security services such as ongoing SIEM log management, vulnerability assessments and real-time incident management via a 24x7 Security Operation Center.

- **Professional Services**

This division drives digital innovation for customers, offering ERP integration, SharePoint and Microsoft solutions, as well as unique products developed by Team Products, such as the Send Secure platform and the Dental Record System (TK2), to optimise business processes.

## Business divisions

In support of these core areas, itm8's business divisions – such as People and Culture, Finance, Marketing, Legal, Internal IT and Compliance & Security – provide a solid base for effective service delivery. These divisions are critical to itm8's operational integrity and ensure that all customer-facing activities are compliant with itm8's standards and regulatory requirements.

Together, these divisions create a robust structure that enables itm8 to provide specialised high-quality services that support customers' strategic goals.

## 3.2. The nature of the processing

The data processor's processing of personal data varies depending on the services contained in the agreement with the data controller and primarily concerns:

### 3.2.1. Hosting and operations

The data processor provides hosting and operating services for the data controller's IT systems and application services. The primary purpose of the processing of personal data is hosting, including the storage of the data controller's personal data as well as the daily operation of IT systems containing personal data. These activities include monitoring, backup and maintenance.

In specific cases, processing activities may include organising, structuring, facilitating, temporarily storing, filtering, troubleshooting, adapting or modifying, retrieving, consulting, using, adapting, combining, restricting or deleting personal data. Such activities are conducted as necessary to provide services to the data controller or to meet specific requests from the data controller.

The data processor also provides IT support to the data controller's employees and other relevant parties. Any support tasks involving the processing of personal data on behalf of the data controller are conducted exclusively at the specific request of the data controller.

### 3.2.2. Support

The data processor provides support to the data controller in connection with the daily operation of the data controller's IT systems. Upon request, the data processor can assume management of the data controller's IT systems, either on-site or via remote access tools like Splashtop or Remote Desktop, to perform specific tasks.

In addition, the data processor can access IT systems to perform troubleshooting and operational activities. In the event of software errors or more extensive problems with the data controller's IT systems, the data processor can retrieve the database from the data controller for troubleshooting, corrections or similar purposes – always by prior agreement.

In certain situations, processing activities may include organising, structuring, facilitating, temporarily storing, filtering, troubleshooting, adapting or modifying, retrieving, consulting, using, adapting, combining, restricting, or deleting personal data. These activities are conducted as necessary to provide the agreed services or fulfil specific requests from the data controller.

### **3.2.3. Consulting services**

The data processor conducts processing in connection with specific, delimited and agreed tasks. The consultancy tasks are conducted on the data controller's systems and data, and the processing will be defined in the specific task.

The tasks are ordered and defined by the data controller, and the data processor participates to the extent necessary in ensuring correct task definition.

### **3.2.4. Database administration**

The data processor provides administration of the data controller's databases and database servers. The primary purpose of the processing is therefore administration, optimisation, maintenance, monitoring and troubleshooting of the data controller's databases containing personal data.

The primary purpose of the processing is not to process personal data, but in connection with the performance of the data processor's obligations, data processing may occur in the data controller's databases.

### **3.2.5. Configuration and development**

The data processor performs tasks related to the development and configuration of the data controller's business applications, including the development of components for ERP systems, CRM, SharePoint and other applications. The tasks are conducted by specific agreement with the data controller.

### **3.2.6. Operation and service of application services**

The data processor provides the data controller with maintenance, configuration, updates, development, support and hosting and operation of the selected application services based on a specific specification with the data controller.

### **3.2.7. Security services**

The data processor performs personal data processing in connection with agreed services on monitoring, setup, reporting, penetration testing and incident management after security breaches.

## **3.3. Personal data**

The personal data that the data processor processes on behalf of the data controller varies between customers. When entering into a data processing agreement, it is the responsibility of the data controller to ensure that the relevant types of personal data and categories of data subjects are correctly defined in the agreements.

## **3.4. Practical measures**

The data processor's level of security reflects a high standard that is adapted to the types of data being processed. Technical and organisational measures are implemented in accordance with the ISO 27001 framework where all controls under ISO 27001 are fully implemented and complied with.

The level of security is also adapted to the specific services described in the agreement between the parties regarding the data processor's provision of services to the data controller. The data processor is both authorised

and obliged to establish the appropriate technical and organisational security measures required to achieve the agreed level of data security. Upon the entry into force of the agreement, it is the responsibility of the data processor to implement and maintain the security measures described in the documents "Organizational and Technical Measures" and "Physical and Logical Security". These documents are available through the data processor's customer portal and at: [legal.itm8.com/compliance](https://legal.itm8.com/compliance).

These security requirements constitute the data controller's overall expectations for security based on the data controller's own risk assessment.

### 3.5. Risk management

As part of the ISO 27001 framework, the data processor adopts a structured approach to risk management. This includes performing risk assessments of implemented controls, data processing activities and vendors (sub-processors).

The risk assessments are based on a probability/consequence model that assesses relevant and probable threats. Threats that achieve a risk score that exceeds the maximum acceptable risk level of the data processor are managed through a risk management plan with the aim of minimising or eliminating the associated risk.

For suppliers, an additional assessment dimension is used in the risk assessments. The data processor includes experience with the supplier's security, including an evaluation of previous security breaches and a review of the supplier's audit report. If the supplier does not provide a standardised audit opinion or if significant findings are identified, follow-up is conducted through a control assessment and, if necessary, through supervision.

The risk assessments are stored and updated regularly and at least once a year.

### 3.6. Control measures

itm8 A/S has implemented the following control measures:

#### 3.6.1. Data processing agreements

The data processor enters into written data processing agreements with both customers and subcontractors. Agreements with customers are based on the data processor's standard agreement which has been prepared based on the Danish Data Protection Agency's standard agreement template.

When a data processing agreement is entered into with a customer, it is archived in the data processor's agreement management system. Any deviations from the standard agreement are documented in this system, and the implementation of the agreement is ensured. New customers must sign a data processing agreement before the data processor starts processing their data. Upon termination of the main agreement, the customer's personal data will, at the customer's choice, either be returned or deleted.

#### 3.6.2. Annual review of procedures

The data processor conducts an annual review of applicable standards and established data processing agreements, or when significant changes occur. This review assesses updating of guidelines and procedures with input from the data processor's legal partner.

As part of the process, suppliers are inspected, reviewed and risk assessed annually. The data processor's supervisory process for sub-processors is based on the Danish Data Protection Agency's point scale and supervision concepts, and each supplier that processes personal data is scored accordingly for this reason. Audit opinions based on applicable standards are obtained from subcontractors where applicable. For suppliers who do not have an audit report, inspections are conducted based on the Danish Data Protection Agency's guidelines.

When the data processor receives a GDPR request, it is managed according to a predefined procedure. The request is processed within 30 days to ensure effective feedback to the data controller or data subject. These requests are documented in the data processor's GRC system.

### 3.6.3. Compliance, roles and responsibilities

Responsibility for information security and compliance at itm8 is anchored at management level. Top management sets the strategic direction and ensures that it is in line with itm8's commitments to quality and regulatory standards. The Compliance & Security department, working under delegation from Management, is responsible for overseeing the implementation, control and continuous improvement of information security and compliance across the organisation.

itm8 is organised into specialised divisions that include both customer-facing and business support functions. The customer-oriented divisions include:

- Managed Services
- Professional Services.

These divisions provide tailored IT services while adhering to itm8's high standards of secure and compliant service delivery. Business support divisions such as People and Culture, Compliance & Security and Internal IT ensure that the basic policies, procedures and frameworks are in place to maintain organisational integrity and security.

Through this structure, the Compliance & Security department ensures that itm8 maintains a coherent approach to risk management and regulatory compliance and information security. At the same time, the department provides ongoing guidance and monitoring to meet the organisation's and customers' requirements. Employees across all divisions are responsible for complying with policies and contributing proactively to a safe environment.

### 3.6.4. Awareness training in relation to GDPR

itm8 prioritises advancing employee knowledge of GDPR compliance across the organisation. Although only a portion of employees regularly manage personal data, itm8 ensures that all employees are informed about proper data handling.

New hires receive training on itm8's information security policies as part of their onboarding process. Updates are provided regularly through internal communication channels, including intranets and news platforms. Ongoing awareness initiatives such as blog posts and posters highlight current security threats and reinforce data protection best practices.

Employees are responsible for complying with itm8's policies and guidelines and contributing to the organisation's commitment to protecting personal data.



### 3.6.5. Monitoring

Access to personal data is limited to authorised users based on a work-related need. User access rights are reviewed annually for standard accounts, while quarterly audits are conducted for privileged accounts.

All access to customer systems by itm8's staff is logged, capturing details such as timestamp, user, privileges and the system that was accessed. These logs are kept for at least six months before they are securely deleted. The logging requirements include:

- Management platform login for access to customer systems
- Login to customer servers
- Login to specific systems and services provided by itm8.

The User Management department conducts several audits throughout the year to ensure compliance with access control policies.

### 3.6.6. Reporting to Management

Management is responsible for information security at itm8 and ensures compliance with organisational goals and regulatory requirements. The Compliance & Security department regularly provides reports to Management on IT security, information security and handling of personal data.

Management is responsible for itm8's data security policies, and Compliance & Security is responsible for ensuring that necessary procedures and instructions are implemented to meet the objectives of the policies. These policies are reviewed at least annually to maintain relevance and effectiveness.

Risk assessments of critical information and data security issues are conducted on an ongoing basis in collaboration with Management and integrate GDPR compliance as a core component of itm8's information security management system.

### 3.6.7. Supervision of sub-processors

ITM8 ensures that approved sub-processors comply with security and regulatory requirements through regular monitoring. This includes obtaining annual IT audit reports such as ISAE 3402 or ISAE 3000 conducted by independent third parties. If these reports are not provided, itm8 applies a risk-based approach based on the Danish Data Protection Agency's guidance on supervision of sub-processors and conducts on-site audits to verify compliance.

itm8 uses its subsidiaries, itm8 Philippines Inc. and itm8 Prague S.R.O, as sub-processors to support service delivery in collaboration with the Danish organisation. These units manage services such as operations, service desk support, development and consulting, including 24/7 monitoring and alarm management.

itm8 Philippines Inc. and itm8 Prague S.R.O are 100% integrated and managed from the Danish organisation and follow the same safety guidelines and instructions.

itm8 Philippines Inc. and itm8 Prague S.R.O are used exclusively for the processing of the personal data of data controllers for customers who have consented to these sub-processors.

### 3.6.8. Categories of personal data collected, processed and stored

As a data processor for the customer (the data controller), itm8 processes personal data exclusively on the customer's instructions. These conditions and the specific categories of personal data are described in the data processing agreements that itm8 enters with its customers. The primary categories of personal data are managed in the customer's applications and systems. ITM8 does not require access to these systems for debugging or operational tasks.

itm8 maintains a list of internal systems where personal data is processed and stored. This list is updated regularly to reflect changes in the workforce and ensure compliance with the requirements of the GDPR and the Danish Bookkeeping Act. Personal data is deleted as soon as it is no longer needed in accordance with these rules.

### 3.6.9. Transfer to third countries

Unless otherwise stated in the customer's specific data processing agreement, personal data will not be transferred to third countries outside the European Union. itm8 only uses its data centres in Denmark for storage and processing. For public cloud services, itm8 uses only European nodes, ensuring compliance with European data protection requirements.

### 3.6.10. Handling security breaches

In the event of a security breach involving a customer system or an internal system where personal data is processed, a case will be opened in itm8's service management system. itm8 will notify the customer within the agreed time of the nature, extent and preliminary assessment of the breach. If itm8 processes personal data on behalf of and in accordance with instructions from the data controller, itm8 will assist in assuming the following responsibilities:

- To support the data controller's notification to the Danish Data Protection Agency of a personal data breach without undue delay and, where possible, no later than 72 hours after the breach has been discovered.
- To support the data controller's information to the data subjects without undue delay if the breach involves a high risk to their rights and freedoms.

### **3.6.11. Significant changes**

There have been no significant changes to procedures and controls in the period from 1 January 2025 to 31 December 2025.

Please refer to section 4 for further description of control objectives and procedures.

## **3.7. Complementary controls at the level of data controllers**

The data controllers have the following obligations:

- Ensure that personal data is up-to-date and correct
- Ensure the legality of instructions in accordance with applicable privacy regulations
- Review and confirm that the instructions in the data processing agreement are correct and contact itm8 if changes are necessary
- Ensure that the personal data being processed, as well as the categories of data subjects, are accurately stated in the data processing agreement
- Ensure that the data controller's users are regularly reviewed and have the correct access profiles
- Perform risk analyses of data subjects at the data controllers
- Conduct audits of their data processors, including itm8
- Continuously review the agreed security measures and configurations for the customer's environment to ensure that they are adequate.

## 4. Control objectives, control activity, tests and test results

### Control objective A:

Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with in accordance with the data processing agreement entered into.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
A.1	<p>Written procedures are in place which include a requirement that personal data must only be processed when instructions to this effect are available.</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>Checked by way of inspection that formalised procedures are in place to ensure that personal data are only processed according to instructions.</p> <p>Checked by way of inspection that the procedures include a requirement to assess at least once a year the need for updates, including in case of changes in the data controller's instructions or changes in the data processing.</p> <p>Checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	Checked by way of inspection that Management ensures that personal data are only processed according to instructions.	No exceptions noted.
A.3	The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions.	<p>Checked by way of inspection that formalised procedures are in place, ensuring verification that personal data are not processed against the Data Protection Regulation or other legislation.</p> <p>Checked by way of inspection that procedures are in place for informing the data controller of cases where the processing of personal data is considered to be against legislation.</p> <p>Checked by way of inspection that the data controller was informed in cases where the processing of personal data was evaluated to be against legislation.</p>	No exceptions noted.

**Control objective B:**

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
B.1	<p>Written procedures are in place which include a requirement that security measures agreed are established for the processing of personal data in accordance with the agreement with the data controller.</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>Checked by way of inspection that formalised procedures are in place to ensure establishment of the security measures agreed.</p> <p>Checked by way of inspection that procedures are up to date.</p> <p>Checked by way of inspection of a sample of data processing agreements that the security measures agreed have been established.</p>	No exceptions noted.
B.2	<p>The data processor has performed a risk assessment and, based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the security measures agreed with the data controller.</p>	<p>Checked by way of inspection that formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security.</p> <p>Checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data.</p> <p>Checked by way of inspection that the data processor has implemented the technical measures ensuring an appropriate level of security consistent with the risk assessment.</p> <p>Checked by way of inspection that the data processor has implemented the security measures agreed with the data controller.</p>	No exceptions noted.
B.3	<p>For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.</p>	<p>Checked by way of inspection that antivirus software has been installed for the systems and databases used in the processing of personal data.</p> <p>Checked by way of inspection that antivirus software is up to date.</p>	No exceptions noted.

**Control objective B:**

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	<p>Checked by way of inspection that external access to systems and databases used in the processing of personal data takes place only through a secured firewall.</p> <p>Checked by way of inspection that the firewall has been configured in accordance with the relevant internal policy.</p>	No exceptions noted.
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	<p>Inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.</p> <p>Inspected network diagrams and other network documentation to ensure appropriate segmentation.</p>	No exceptions noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	<p>Checked by way of inspection that formalised procedures are in place for restricting users' access to personal data.</p> <p>Checked by way of inspection that formalised procedures are in place for following up on users' access to personal data being consistent with their work-related need.</p> <p>Checked by way of inspection that the technical measures agreed support retaining the restriction in users' work-related access to personal data.</p> <p>Checked by way of inspection of a sample of users' access to systems and databases that such access is restricted to the employees' work-related need.</p>	No exceptions noted.

**Control objective B:**

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
B.7	<p>System monitoring with an alarm feature has been established for the systems and databases used in the processing of personal data. This monitoring comprises:</p> <ul style="list-style-type: none"> <li>• User login</li> <li>• Critical settings of systems and databases.</li> </ul>	<p>Checked by way of inspection that system monitoring with an alarm feature has been established for systems and databases used in the processing of personal data.</p> <p>Checked by way of inspection of a sample of alarms that these were followed up on and monitored.</p>	No exceptions noted.
B.8	<p>Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.</p>	<p>Checked by way of inspection that formalised procedures are in place to ensure that transmissions of sensitive and confidential personal data through the internet are protected by strong encryption based on a recognised algorithm.</p> <p>Checked by way of inspection that technological encryption solutions have been available and active throughout the assurance period.</p> <p>Checked by way of inspection that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.</p> <p>Inquired whether any unencrypted transmission of sensitive and confidential personal data has taken place during the assurance period and whether the data controllers have been appropriately informed thereof.</p>	No exceptions noted.

**Control objective B:**

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
B.9	<p>Logging of the following matters has been established in systems, databases and networks:</p> <ul style="list-style-type: none"> <li>• Activities performed by system administrators and others holding special rights</li> <li>• Security incidents comprising:               <ul style="list-style-type: none"> <li>○ Changes in log set-ups, including disabling of logging</li> <li>○ Changes in users' system rights</li> <li>○ Failed attempts to log on to systems, databases or networks.</li> </ul> </li> </ul> <p>Log data are protected against manipulation and technical errors and are reviewed regularly.</p>	<p>Checked by way of inspection that formalised procedures are in place for setting up logging of user activities in systems, databases or networks that are used to process and transmit personal data, including review of and follow-up on logs.</p> <p>Checked by way of inspection that logging of user activities in systems, databases or networks that are used to process or transmit personal data has been configured and activated.</p> <p>Checked by way of inspection that user activity data collected in logs are protected against manipulation or deletion.</p> <p>Checked by way of inspection of a sample of logging that the content of log files is as expected compared to the set-up and that documentation confirms the follow-up performed and the response to any security incidents.</p> <p>Checked by way of inspection of a sample of logging that documentation confirms the follow-up performed on activities carried out by system administrators and others holding special rights.</p>	No exceptions noted.

**Control objective B:**

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.	<p>Checked by way of inspection that formalised procedures are in place for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised form.</p> <p>Checked by way of inspection of a sample of development or test databases that personal data included therein are pseudonymised or anonymised.</p> <p>Checked by way of inspection of a sample of development or test databases in which personal data are not pseudonymised or anonymised that this has taken place according to agreement with, and on behalf of, the data controller.</p>	No exceptions noted.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	<p>Checked by way of inspection that formalised procedures are in place for regularly testing technical measures, including for performing vulnerability scans and penetration tests.</p> <p>Checked by way of inspection of samples that regular testing of the technical measures established is documented.</p> <p>Checked by way of inspection that any deviations or weaknesses in the technical measures have been attended to in a timely and satisfactory manner and communicated to the data controllers as appropriate.</p>	No exceptions noted.

**Control objective B:**

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
B.12	Changes to systems, databases or networks are made consistently with established procedures that ensure maintenance using relevant updates and patches, including security patches.	<p>Checked by way of inspection that formalised procedures are in place for handling changes to systems, databases or networks, including handling of relevant updates, patches and security patches.</p> <p>Checked by way of inspection of extracts from technical security parameters and set-ups that systems, databases or networks have been updated using agreed changes and relevant updates, patches and security patches.</p>	<p>During our audit, we found that the existing procedural framework for change management has not been fully comprehensive across all of Managed Services, as different ITSM systems have been used during the period.</p> <p>Furthermore, during our review of one of the selected customers' server environments, it was identified that one out of three audited MSSQL servers for the customer had not been sufficiently patched.</p>
No further deviations noted.			
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	<p>Checked by way of inspection that formalised procedures are in place for granting and removing users' access to systems and databases used for processing personal data.</p> <p>Checked by way of inspection of a sample of employees' access to systems and databases that the user accesses granted have been authorised and that a work-related need exists.</p> <p>Checked by way of inspection of a sample of resigned or dismissed employees that access to systems and databases was deactivated or removed in a timely manner.</p> <p>Checked by way of inspection that documentation states that user accesses granted are evaluated and authorised on a regular basis – and at least once a year.</p>	<p>During our audit, we found that the executed user-management controls were not documented sufficiently in accordance with the applicable procedures. Furthermore, documentation was not available for all periodic reviews of privileged user access for two management domains.</p> <p>We have been informed that the controls were performed, but they were not documented. In our samples, we did not identify any deviations</p> <p>No further deviations noted.</p>

**Control objective B:**

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
B.14	Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication.	<p>Checked by way of inspection that formalised procedures are in place to ensure that two-factor authentication is applied in the processing of personal data that involves a high risk for the data subjects.</p> <p>Checked by way of inspection that users' access to processing personal data that involve a high risk for the data subjects may only take place by using two-factor authentication.</p>	No exceptions noted.
B.15	Physical access security measures have been established so as to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed.	<p>Checked by way of inspection that formalised procedures are in place to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed.</p> <p>Checked by way of inspection of documentation that, throughout the assurance period, only authorised persons have had physical access to premises and data centres at which personal data are stored and processed.</p>	No exceptions noted.

**Control objective C:**

Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
C.1	<p>Management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The information security policy is based on the risk assessment performed.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the information security policy should be updated.</p>	<p>Checked by way of inspection that an information security policy exists that Management has considered and approved within the past year.</p> <p>Checked by way of inspection of documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.</p>	No exceptions noted.
C.2	<p>Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.</p>	<p>Inspected documentation of Management's assessment that the information security policy generally meets the requirements for security measures and the security of processing in the data processing agreements entered into.</p> <p>Checked by way of inspection of a sample of data processing agreements that the requirements therein are covered by the requirements of the information security policy for security measures and security of processing.</p>	No exceptions noted.

**Control objective C:**

Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
C.3	The employees of the data processor are screened as part of the employment process. Such screening consists of certificates of criminal record.	<p>Checked by way of inspection that formalised procedures are in place to ensure screening of the data processor's employees as part of the employment process.</p> <p>Checked by way of inspection of a sample of data processing agreements that the requirements therein for screening employees are covered by the data processor's screening procedures.</p> <p>Checked by way of inspection of employees appointed during the assurance period that documentation states that the screening has comprised:</p> <ul style="list-style-type: none"> <li>• References from former employers</li> <li>• Certificates of criminal record</li> <li>• Diplomas.</li> </ul>	No exceptions noted.
C.4	Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.	<p>Checked by way of inspection of employees appointed during the assurance period that the relevant employees have signed a confidentiality agreement.</p> <p>Checked by way of inspection of employees appointed during the assurance period that the relevant employees have been introduced to:</p> <ul style="list-style-type: none"> <li>• The information security policy</li> <li>• Procedures for processing data and other relevant information.</li> </ul>	No exceptions noted.

**Control objective C:**

Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
C.5	For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned.	<p>Inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal and that assets such as access cards, computers, mobile phones, etc. are returned.</p> <p>Checked by way of inspection of employees resigned or dismissed during the assurance period that rights have been deactivated or terminated and that assets have been returned.</p>	No exceptions noted.
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	<p>Checked by way of inspection that formalised procedures are in place to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality.</p> <p>Checked by way of inspection of employees resigned or dismissed during the assurance period that documentation confirms the continued validity of the confidentiality agreement and the general duty of confidentiality.</p>	No exceptions noted.
C.7	Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data.	<p>Checked by way of inspection that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data.</p> <p>Inspected documentation stating that all employees who have either access to or process personal data have completed the awareness training provided.</p>	No exceptions noted.

**Control objective D:**

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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
D.1	<p>Written procedures are in place which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller.</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>Checked by way of inspection that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller.</p> <p>Checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
D.2	<p>The following specific requirements have been agreed with respect to the data processor's storage periods and deletion routines:</p> <ul style="list-style-type: none"> <li>• Data in the customer's systems and configurations in firewalls etc. will be deleted no earlier than one month after and no later than three months after the termination of the agreement.</li> <li>• Data about the customer in itm8's systems and where itm8 is data controller will be deleted based on the current deletion deadline for the individual system.</li> </ul>	<p>Checked by way of inspection that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines.</p> <p>Checked by way of inspection of a sample of data processing sessions from the data processor's list of processing activities that documentation states that personal data are stored in accordance with the agreed storage periods.</p> <p>Checked by way of inspection of a sample of data processing sessions from the data processor's list of processing activities that documentation states that personal data are deleted in accordance with the agreed deletion routines.</p>	No exceptions noted.
D.3	<p>Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been:</p> <ul style="list-style-type: none"> <li>• Returned to the data controller and/or</li> <li>• Deleted if this is not in conflict with other legislation.</li> </ul>	<p>Checked by way of inspection that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data.</p> <p>Checked by way of inspection of terminated data processing sessions during the assurance period that documentation states that the agreed deletion or return of data has taken place.</p>	No exceptions noted.

**Control objective E:**

Procedures and controls are complied with to ensure that the data processor will only store personal data in accordance with the agreement with the data controller.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
E.1	<p>Written procedures are in place which include a requirement that personal data must only be stored in accordance with the agreement with the data controller.</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>Checked by way of inspection that formalised procedures are in place for only storing and processing personal data in accordance with the data processing agreements.</p> <p>Checked by way of inspection that procedures are up to date.</p> <p>Checked by way of inspection of a sample of data processing sessions from the data processor's list of processing activities that documentation states that data processing takes place in accordance with the data processing agreement.</p>	No exceptions noted.
E.2	<p>Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.</p>	<p>Checked by way of inspection that the data processor has a complete and updated list of processing activities stating localities, countries or regions.</p> <p>Checked by way of inspection of a sample of data processing sessions from the data processor's list of processing activities that documentation states that the processing of data, including the storage of personal data, takes place only in the localities stated in the data processing agreement – or otherwise as approved by the data controller.</p>	No exceptions noted.

**Control objective F:**

Procedures and controls are complied with to ensure that only approved subprocessors 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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
F.1	<p>Written procedures are in place which include requirements for the data processor when using subprocessors, including requirements for subprocessing agreements and instructions.</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>Checked by way of inspection that formalised procedures are in place for using subprocessors, including requirements for subprocessing agreements and instructions.</p> <p>Checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
F.2	<p>The data processor only uses subprocessors to process personal data that have been specifically or generally approved by the data controller.</p>	<p>Checked by way of inspection that the data processor has a complete and updated list of subprocessors used.</p> <p>Checked by way of inspection of a sample of subprocessors from the data processor's list of subprocessors that documentation states that the processing of data by the subprocessor follows from the data processing agreements – or otherwise as approved by the data controller.</p>	No exceptions noted.
F.3	<p>When changing the generally approved subprocessors 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 subprocessors used, this has been approved by the data controller.</p>	<p>Checked by way of inspection that formalised procedures are in place for informing the data controller when changing the subprocessors used.</p> <p>Inspected documentation stating that the data controller was informed when changing the subprocessors used throughout the assurance period.</p>	No exceptions noted.

**Control objective F:**

Procedures and controls are complied with to ensure that only approved subprocessors 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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
F.4	The data processor has subjected the subprocessor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	<p>Checked by way of inspection for existence of signed subprocessing agreements with subprocessors used, which are stated on the data processor's list.</p> <p>Checked by way of inspection of a sample of subprocessing agreements that they include the same requirements and obligations as are stipulated in the data processing agreements between the data controllers and the data processor.</p>	No exceptions noted.
F.5	<p>The data processor has a list of approved subprocessors disclosing:</p> <ul style="list-style-type: none"> <li>• Name</li> <li>• Company registration no.</li> <li>• Address</li> <li>• Description of the processing.</li> </ul>	<p>Checked by way of inspection that the data processor has a complete and updated list of subprocessors used and approved.</p> <p>Checked by way of inspection that, as a minimum, the list includes the required details about each subprocessor.</p>	No exceptions noted.

**Control objective F:**

Procedures and controls are complied with to ensure that only approved subprocessors 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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
F.6	Based on an updated risk assessment of each subprocessor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the subprocessor.	<p>Checked by way of inspection that formalised procedures are in place for following up on processing activities at subprocessors and compliance with the subprocessing agreements.</p> <p>Checked by way of inspection of documentation that each subprocessor and the current processing activity at such processor are subjected to risk assessment.</p> <p>Checked by way of inspection of documentation that technical and organisational measures, security of processing at the subprocessors used, third countries' bases of transfer and similar matters are appropriately followed up on.</p> <p>Checked by way of inspection of documentation that information on the follow-up at subprocessors is communicated to the data controller so that such controller may plan an inspection.</p>	No exceptions noted.

**Control objective G:**

Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
G.1	<p>Written procedures are in place which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.</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>Checked by way of inspection that formalised procedures are in place to ensure that personal data are only transferred to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.</p> <p>Checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
G.2	<p>The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.</p>	<p>Checked by way of inspection that the data processor has a complete and updated list of transfers of personal data to third countries or international organisations.</p> <p>Checked by way of inspection of a sample of data transfers from the data processor's list of transfers that documentation states that such transfers were arranged with the data controller in the data processing agreement or subsequently approved.</p>	No exceptions noted.
G.3	<p>As part of the transfer of personal data to third countries or international organisations, the data processor assessed and documented the existence of a valid basis of transfer.</p>	<p>Checked by way of inspection that formalised procedures are in place for ensuring a valid basis of transfer.</p> <p>Checked by way of inspection that procedures are up to date.</p> <p>Checked by way of inspection of a sample of data transfers from the data processor's list of transfers that documentation confirms a valid basis of transfer in the data processing agreement with the data controller and that transfers have only taken place insofar as this was arranged with the data controller.</p>	No exceptions noted.

**Control objective H:**

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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
H.1	<p>Written procedures are in place 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>Checked by way of inspection 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>Checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
H.2	<p>The data processor has established procedures that, insofar as this was agreed, 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.</p>	<p>Checked by way of inspection 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>Checked by way of inspection of documentation that the systems and databases used support the performance of the relevant detailed procedures.</p>	No exceptions noted.

**Control objective I:**

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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
I.1	<p>Written procedures are in place which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches.</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>Checked by way of inspection that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches.</p> <p>Checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
I.2	<p>The data processor has established the following controls to identify any personal data breaches:</p> <ul style="list-style-type: none"> <li>• Awareness of employees</li> <li>• Monitoring of network traffic</li> <li>• Follow-up on logging of access to personal data.</li> </ul>	<p>Checked by way of inspection that the data processor provides awareness training to the employees in identifying any personal data breaches.</p> <p>Checked by way of inspection of documentation that network traffic is monitored and that anomalies, monitoring alarms, large file transfers, etc. are followed up on.</p> <p>Checked by way of inspection of documentation that logging of access to personal data, including follow-up on repeated attempts to gain access, is followed up on in a timely manner.</p>	No exceptions noted.

**Control objective I:**

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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
I.3	If any personal data breach occurred, the data processor informed the data controller without undue delay and no later than 72 hours after having become aware of such personal data breach at the data processor or a subprocessor.	<p>Checked by way of inspection that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach.</p> <p>Made inquiries of the subprocessors as to whether they have identified any personal data breaches throughout the assurance period.</p> <p>Checked by way of inspection that the data processor has included any personal data breaches at subprocessors in the data processor's list of security incidents.</p> <p>Checked by way of inspection that all personal data breaches recorded at the data processor or the subprocessors have been communicated to the data controllers concerned without undue delay and no later than 72 hours after the data processor became aware of the personal data breach.</p>	No exceptions noted.

**Control objective I:**

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.

No.	itm8's control activity	Tests performed by PwC	Result of PwC's tests
I.4	<p>The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency. These procedures must contain instructions on descriptions of:</p> <ul style="list-style-type: none"> <li>• The nature of the personal data breach</li> <li>• Probable consequences of the personal data breach</li> <li>• Measures taken or proposed to be taken to respond to the personal data breach.</li> </ul>	<p>Checked by way of inspection that the procedures in place for informing the data controllers in the event of any personal data breach include detailed instructions for:</p> <ul style="list-style-type: none"> <li>• Describing the nature of the personal data breach</li> <li>• Describing the probable consequences of the personal data breach</li> <li>• Describing measures taken or proposed to be taken to respond to the personal data breach.</li> </ul> <p>Checked by way of inspection of documentation that the procedures available support that measures are taken to respond to the personal data breach.</p>	No exceptions noted.

# PENNEO

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

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

## Frank Bech Jensen

### Kunde

Serienummer: 4ecd2cc-e8cb-4f9e-bfb0-5e4b63b8ee2c  
IP: 193.169.xxx.xxx  
2026-02-17 12:35:44 UTC



## Jesper Parsberg Madsen

### PRICEWATERHOUSECOOPERS STATS AUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231 Statsautoriseret revisor

Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e  
IP: 87.49.xxx.xxx  
2026-02-17 12:55:00 UTC



## Iraj Bastar

### PRICEWATERHOUSECOOPERS STATS AUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231 PwC-medunderskriver

Serienummer: 945792b8-522b-4f8c-9f2d-bc89647c3d96  
IP: 208.127.xxx.xxx  
2026-02-17 13:05:11 UTC



Penneo dokumentnøgle: 8AXQW-EWEID-8VYE-JCJT-ENN6E-3FMMIC

Dette dokument er underskrevet digitalt via **Penneo.com**. De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptografiske beviser er indlejret i denne PDF for validering i fremtiden.

Dette dokument er forseglet med et kvalificeret elektronisk segl. For mere information om Penneos kvalificerede tillidstjenester, se <https://eutl.penneo.com>.

### Sådan kan du verificere, at dokumentet er originalt

Når du åbner dokumentet i Adobe Reader, kan du se, at det er certificeret af **Penneo A/S**. Dette beviser, at indholdet af dokumentet er uændret siden underskriftstidspunktet. Bevis for de individuelle underskrivers digitale underskrifter er vedhæftet dokumentet.

Du kan verificere de kryptografiske beviser vha. Penneos validator, <https://penneo.com/validator>, eller andre valideringstjenester for digitale underskrifter.