itm8 A/S

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 January 2024 to 31 December 2024 pursuant to the data processing agreement with data controllers

February 2025

Contents

1. Management's statement

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

The accompanying description has been prepared for data controllers who have used itm8 A/S's hosting services and who have a sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves 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.

itm8 A/S uses B4Restore and Keepit as subprocessors for backup services. This report uses the carve-out method and does not comprise control objectives and related controls that B4Restore and Keepit perform for itm8 A/S.

Some of the control objectives stated in our description in section 3 can only be achieved if the complementary controls at the data controllers are suitably designed and operating effectively with our controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

itm8 A/S confirms that:

a) The accompanying description in section 3 fairly presents information security and measures in relation to the hosting services that have processed personal data for data controllers subject to the data protection rules throughout the period from 1 January 2024 to 31 December 2024. The criteria used in making this statement were that the accompanying description:

   (i) Presents how the information security and measures in relation to the hosting 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 hosting 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 information about changes in the data processor's hosting services for the processing of personal data in the period from 1 January 2024 to 31 December 2024;

(iii) Does not omit or distort information relevant to the scope of the hosting 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 hosting services that the individual data controllers might consider important in their 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 2024 to 31 December 2024. 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; and

(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 2024 to 31 December 2024.

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, 3rd February 2025
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 2024 to 31 December 2024 pursuant to the data processing agreement with data controllers

To: itm8 A/S and itm8 A/S's customers

Scope

We have been engaged to provide assurance about itm8 A/S's description in section 3 of the hosting services in accordance with the data processing agreement with data controllers throughout the period from 1 January 2024 to 31 December 2024 (the description) and about the design and operating effectiveness of controls related to the control objectives stated in the description.

Our report covers whether itm8 A/S 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 A/S'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").

itm8 A/S uses B4Restore and Keepit as subprocessors for backup services. This report uses the carve-out method and does not comprise control objectives and related controls that B4Restore and Keepit perform for itm8 A/S.

Some of the control objectives stated in itm8 A/S's description in section 3 can only be achieved if the complementary controls at the data controllers are suitably designed and operating effectively with itm8 A/S's controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

We express reasonable assurance in our conclusion.

itm8 A/S's responsibilities

itm8 A/S is responsible for: preparing the description and accompanying statement in section 1, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives and designing and effectively operating controls to achieve the stated control objectives.

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 itm8 A/S's description and on the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures.

We 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, design and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of its hosting services and about the design and operating effectiveness of controls. The procedures selected depend on the auditor's judgement, including the assessment of the 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 the Management's statement section.

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

Limitations of controls at a data processor

itm8 A/S'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 hosting services that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect all personal data breaches. Furthermore, the projection of any evaluation of the operating effectiveness to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the Management's statement section. In our opinion, in all material respects:

a) The description fairly presents the information security and measures in relation to the hosting services as designed and implemented throughout the period from 1 January 2024 to 31 December 2024;

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 January 2024 to 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, operated effectively throughout the period from 1 January 2024 to 31 December 2024.

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

This report and the description of tests of controls in section 4 are intended only for data controllers who have used itm8 A/S's hosting services and who have a sufficient understanding to consider it, along with other information, including information about controls operated by the data controllers themselves, in assessing whether the requirements of the data protection rules have been complied with.

Aarhus, 3rd February 2025
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

Iraj Bastar
Director

3. Description of processing

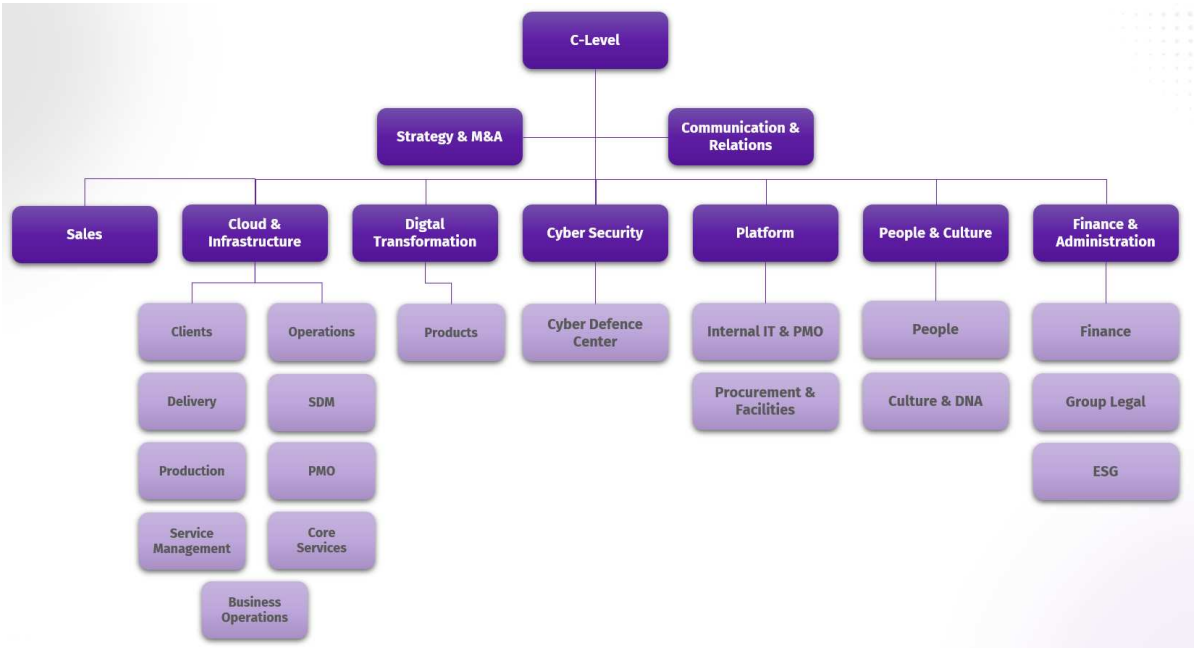
The purpose of the data processor's activities in processing personal data on behalf of the data controller is to deliver the agreed services outlined in the contracts between the data controller and the data processor. These services encompass Hosting and Operations, Service Desk, Application Services and Consultancy Services. The data processing instructions provided by the data controller are clearly defined within the data processor agreement between the respective partners. This framework ensures that the processing activities are aligned with the contractual obligations and regulatory requirements.

Description of the service organisation

itm8 A/S has undergone rapid development to become a structured organisation delivering specialised IT services and solutions. itm8 is organised into several divisions, including both customer-facing divisions that drive service delivery and business divisions that provide essential administrative and operational support. This setup enables itm8 to offer integrated, reliable services that meet high standards of quality and compliance for a diverse client base.

This independent assurance report is focused on itm8 | Cloud & Infrastructure, which is included as the scope of this report. The division provides cloud solutions and IT infrastructure services that align with itm8's standards for quality and secure service delivery. Additionally, the scope includes specific components from itm8 | Cybersecurity, particularly the Cyber Defense Center, which delivers 24/7 monitoring, SIEM log management and incident response essential to infrastructure security.

Further, the report includes elements of itm8 | Digital Transformation, specifically the Team Products group, which develops custom solutions such as Send Secure (SEPO) and the Dental Records system (TK2). These specialised solutions support itm8's commitment to secure, tailored services that meet clients' unique operational needs.



Scope of the itm8 | Cloud & Infrastructure Independent assurance report

Customer divisions

The customer-facing divisions are itm8's primary service pillars, each dedicated to specific areas of expertise:

- **itm8 | Cloud & Infrastructure**
  Focused on cloud solutions and IT infrastructure, this division helps customers implement robust hosting and operational strategies. It transforms client business strategies into scalable cloud and infrastructure solutions through platform assessments, security policy design, migrations, modernization and 24/7 support.

- **itm8 | Cybersecurity**
  Offering comprehensive security services, itm8 | Cybersecurity spans everything from penetration testing and red teaming to cyber risk consultancy. It includes a Cyber Defence Center for continuous SIEM log management, vulnerability assessments and real-time incident response.

- **itm8 | Digital Transformation**
  This division drives digital innovation for clients, offering ERP integration, SharePoint and Microsoft solutions along with unique products developed by Team Products, such as the Send Secure platform and Dental Records system (TK2), to optimise business processes.

- **itm8 | Application Services**
  itm8's Application Services division accelerates application development and maintenance with a focus on security and quality. Services include application management, database administration, monitoring, performance tuning and technical support.

Business divisions

Supporting these pillars, itm8's business divisions—such as HR, Marketing, Legal, Internal IT and Compliance & Security—provide the foundation for effective service delivery. These divisions are integral to itm8's operational integrity and ensure that all customer-facing activities align with itm8's standards and regulatory requirements.

Together, these divisions create a robust structure that enables itm8 to deliver specialised, high-quality services aligned with clients' strategic goals.

Nature of processing

The data processor's processing of personal data on behalf of the data controller primarily concerns:

Hosting and operation

The data processor provides hosting and operational services for the data controller's IT systems and application services. The primary purpose of personal data processing is hosting, including the storage of the data controller's personal data, as well as the day-to-day operation of IT systems containing personal data. These operations encompass monitoring, backup and maintenance.

In specific instances, data processing activities may include organising, structuring, facilitating, temporary storage, filtering, troubleshooting, adapting or altering, retrieving, consulting, using, aligning, combing, restricting or erasing personal data. Such activities are conducted as necessary to deliver services to the data controller or to comply with specific requests made by the data controller.

The data processor also provides IT support to the data controller's employees and other relevant parties. Any support-related tasks involving the processing of personal data on behalf of the data controller are carried out solely upon the data controller's specific request.

Service desk

The data processor provides support to the data controller for the day-to-day operation of the data controller's IT systems. Upon request, the data processor may assume management of the data controller's IT systems, either on-site or via remote access tools such as TeamViewer or Remote Desktop to complete specific tasks.

Additionally, the data processor may access IT systems to perform troubleshooting and operational activities. In the event of software failures or broader issues with the data controller's IT systems, the data processor may retrieve the database from the data controller for troubleshooting, corrections or similar purposes, always subject to prior agreement.

In certain situations, data processing activities may involve organising, structuring, facilitating, temporary storage, filtering, troubleshooting, adapting or altering, retrieving, consulting, using, aligning, combining, restricting or erasing personal data. These activities are conducted as necessary to deliver the agreed services or to fulfil specific requests from the data controller.

Application services

The data processor supplies support, operation, backup and application maintenance services for applications it has developed in-house. Two key applications included in this service are:

SEPO – Secure Mail

SEPO is a secure mail application developed by the data processor. The service includes:

- Encryption, decryption, signing and forwarding of emails, as well as digital mail (Digital Post) or electronic post-box notices (e-Boks) to and from the data controller
- Secure storage of the data controller's cryptographic key(s).

TK2 EPJ

TK2 EPJ, an IT system also developed by the data processor, is maintained and supported as part of this service. Any work involving the processing of personal data is carried out only at the specific request of the data controller.

Support is delivered via remote access tools such as TeamViewer. Upon request, the data processor may temporarily take over the management of the system via TeamViewer to address specific tasks. In the event of product failures, the data processor may obtain the TK2 SQL database from the data controller for troubleshooting, corrections or similar purposes.

In certain cases, data processing activities may include organising, structuring, facilitating, temporary storage, filtering, troubleshooting, adapting or altering, retrieving, consulting, using, aligning, combining, restricting or erasing personal data. These actions are performed as required to deliver the agreed services or to fulfil specific requests from the data controller.

Consultancy services

The data processor provides specific and limited consultancy services. These tasks are performed within the data controller's systems and involve the data controller's data. The scope and nature of processing activities are defined for each individual task.

Consultancy assignments are initiated and outlined by the data controller, with the data processor offering assistance as needed to ensure tasks are properly defined and aligned with the data controller's requirements.

Personal data

The personal data processed by the data processor on behalf of the data controller varies between customers.

When establishing a data processing agreement, it is the responsibility of the data controller to ensure that the appropriate types of personal data and categories of data subjects are accurately defined with the agreements.

Practical measures

The level of security maintained by the data processor reflects a generally high standard, tailored to the types of data being processed. Technical and organisational measures are implemented in accordance with the ISO 27001 security framework, with all controls under ISO 27001 fully implemented and adhered to.

The security level is further aligned with the specific services outlined in the agreement between the parties concerning the data processor's provision of services to the data controller. The data processor is both authorised and obligated to determine the appropriate technical and organisational security measures required to achieve the agreed-upon level of data security.

Upon commencement of the agreement, the data processor is responsible for implementing and maintaining the security measures detailed in the documents "Organizational and Technical Measures" and "Physical and Logical Security". These documents are accessible via the data processor's customer portal and at: legal.itm8.com/compliance

These security requirements constitute the data controller's comprehensive expectations regarding security, based on the data controller's own risk assessment.

Risk assessment

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

Risk assessments are based on a probability/consequence model, evaluating relevant and likely threats. Threats receiving a risk score exceeding the data processor's maximum risk acceptance are addressed through a risk treatment plan, aiming to minimise or eliminate the associated risk.

For suppliers, an additional perspective is applied during risk assessments. The data processor incorporates its experience with the supplier's security, including an evaluation of past security breaches and a review of the supplier's audit report. If the supplier does not provide a standard audit report or if significant findings are identified, follow-up is conducted using a control assessment from and, if necessary, through supervision.

Risk assessments are reviewed and updated regularly, with a minimum frequency of once per year.

There have been no significant changes to procedures and controls in the period from 1 January 2024 to 31 December 2024.

Control measures

itm8 A/S has implemented the following control measures:

Data processor agreements

The data processor establishes written data processor agreements with both customers and subcontractors. Agreements with customers are based on the data processor's standard data processor agreement, which is derived from the Danish Data Protection Agency's standard template.

When a data processor 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 within this system, and the implementation of the agreement is ensured. New customers are required to sign a data processor agreement before the data processor begins processing their data.

Yearly review of procedures

The data processor conducts an annual review of applicable standards and established data processor agreements or whenever significant changes occur. This review evaluates updates to guidelines and procedures, with input from the data processor's legal partner.

As part of this process, suppliers are inspected, reviewed and risk assessed annually. Audit reports based on current standards are obtained from subcontractors. For suppliers lacking an audit report, extended supervision is conducted.

When the data processor receives a GDPR inquiry, it is handled following a predefined procedure. The inquiry is processed within 30 days, ensuring effective feedback to the data controller or data subject. These inquiries are documented in the IT Service Management (ITSM) system.

Compliance, roles and responsibilities

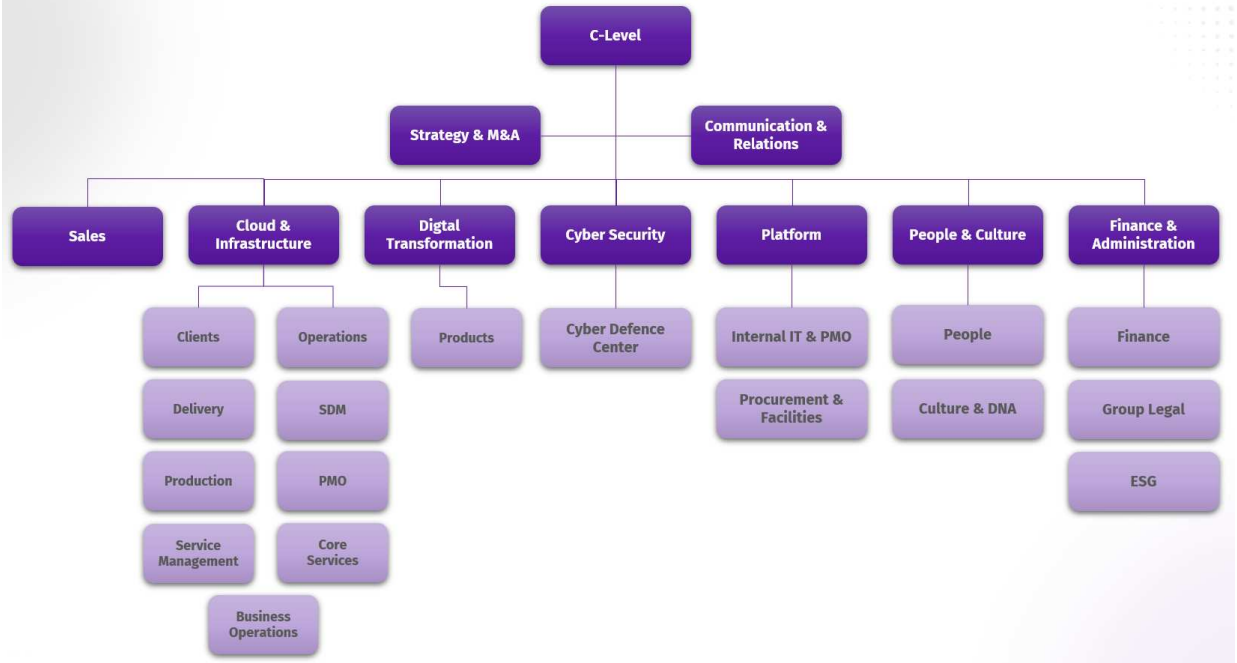
Responsibility for information security and compliance within itm8 is anchored at the leadership level. Top management defines the strategic direction and ensures alignment with itm8's commitment to quality and regulatory standards. The Compliance & Security department, under delegation from leadership, is responsible for overseeing the implementation, control and continuous improvement of information security and compliance across the organisation.

Itm8 is structed into specialised divisions, encompassing both customer-facing and business support functions. Customer-facing divisions, include:

- itm8 | Coud & Infrastructure
- itm8 | Cybersecurity
- itm8 | Digital Transformation.

These deliver tailored IT services while adhering to itm8's high standards for secure and compliant service delivery. Business support divisions such as HR, Compliance & Security and Internal IT ensure the foundational policies, procedures and frameworks are in place to uphold organisational integrity and security.

Through this structure, the Compliance & Security department ensures that itm8 maintains a cohesive approach to risk management, regulatory compliance and information security while providing ongoing guidance and monitoring to meet organisational and client requirements. Employees across all divisions are responsible for adhering to these policies and proactively contributing to a secure environment.



Scope of the itm8 | Cloud & Infrastructure Independent assurance report

Employee awareness in relation to the GDPR

Itm8 prioritises fostering employee awareness of GDPR compliance across the organisation. While only a portion of employees regularly handle person data, itm8 ensures all staff are informed about proper data handling practices.

New employees receive training on itm8's information security policies during their onboarding process. Regularly updates are provided through internal communication channels, including intranet and news platforms. Monthly 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, contributing to the organisation's commitment to safeguarding personal data.

Monitoring

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

All access to customer systems by itm8 personnel is logged, capturing details such as timestamp, user, privileges and the system accessed. These logs are retained for at least six months before being securely deleted. Logging requirements include:

- Login to the administration platform 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 adherence to access control policies.

Reporting to Management

The Executive Management Team (EMT) oversees information security across itm8, ensuring alignment with organisational goals and regulatory requirements. The Compliance & Security department provides regular reports to the MET on IT security, information security and the handling of personal data.

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

Risk assessments on critical information and data security matters are conducted on an ongoing basis in collaboration with the EMT, integrating GDPR compliance as a core component of itm8's information security management system.

Supervision with sub-processors

itm8 ensures that approved sub-processors maintain compliance with security and regulatory requirements through regular monitoring. This includes obtaining annual IT audit reports, such as ISAE 3402 or ISAE 3000, performed by independent third parties. If these reports are not provided, itm8 applies a risk-based approach, conducting on-site audits to verify compliance.

itm8 leverages 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 entities handle services such as operations, service desk support, development and consultancy, 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 have the same security guidelines and instructions.

itm8 Philippines Inc. and itm8 Prague S.R.O are exclusively used for the processing of the data controller's personal data for customers who have accepted them as subprocessor.

Categories of personal data collected, processed and stored

As a data processor for the customer (data controller), itm8 collects, processes and stores personal data solely at the customer's direction. These matters and the specific categories of personal data are detailed in the data processing agreements into which itm8 enters with its customers. The primary categories of personal data are managed within customer applications and systems. Itm8 does not require access to these systems for bug fixes or operational tasks.

Itm8 maintains a list of internal systems where personal data is processed and stored. This list is regularly updated to reflect changes in the workforce and ensures 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 regulations.

Transfer to third countries

Unless otherwise specified in the customer's specific data processing agreement, personal data will not be transferred to third countries outside the European Union. Itm8 uses only its data centres located in Denmark for storage and processing. For public cloud services, itm8 utilises European nodes exclusively, ensuring compliance with European data protection requirements.

Handling of security breaches

In the event of security breaches involving a customer system or an internal system where personal data is processed, a ticket will be opened in itm8's service management system. Itm8 will notify the customer within the agreed timeframe about the nature, scale and preliminary extent of the breach. If itm8 is processing personal data on behalf of and following instructions from the data controller, it will assist in assuming the following responsibilities:

- Reporting a personal data breach to the Danish Data Protection Agency without undue delay, and where feasible, no later than 72 hours after becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons

- Informing the data subject(s) without undue delay if the breach involves a high risk to their rights and freedoms

- Consulting with the Danish Data Protection Agency before processing if a data protection impact assessment indicates that processing could result in a high risk due to the measures taken by the data controller to mitigate that risk.

Control objectives and activities are detailed in section 4.

Complementary controls at the data controllers

The data controllers have the following obligations:

- Ensure that personal data is up to date
- Ensure the legality of instruction in accordance with current privacy regulations
- Revie and confirm that instructions in the data processing agreement are correct and contact itm8 if changes are needed
- Ensure that the types of personal data and categories of data subjects are accurate in the data processing agreement
- Ensure that the data controller's users are regularly reviewed and have the correct access profiles
- Perform risk analyses on the controllers' data subjects
- Conduct audits of their data processors, including itm8
- Continuously review the agreed safety measures and configurations for the customer's environment to ensure 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.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
A.1	Written procedures are in place which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place to ensure that personal data are only processed according to instructions. 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. Checked by way of inspection that procedures are up to date.	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. Checked by way of inspection of personal data processing operation for sample testing of data processing agreements that the processing is conducted consistently with instructions.	No exceptions noted.

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.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
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.	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. 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. 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.	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.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
B.1	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. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place to ensure establishment of the security measures agreed. Checked by way of inspection that procedures are up to date. Checked by way of inspection of samples of data processing agreements that the security measures agreed have been established.	No exceptions noted.
B.2	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.	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. Checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data. 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. Checked by way of inspection that the data processor has implemented the security measures agreed with the data controller.	No exceptions noted.
B.3	For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.	Checked by way of inspection that antivirus software has been installed for the systems and databases used in the processing of personal data. Checked by way of inspection that antivirus software is up to date.	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.	Data processor'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.	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. Checked by way of inspection that the firewall has been configured in accordance with the relevant internal policy.	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.	Inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. Inspected network diagrams and other network documentation to ensure appropriate segmentation.	No exceptions noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	Checked by way of inspection that formalised procedures are in place for restricting users' access to personal data. 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. Checked by way of inspection that the technical measures agreed support retaining the restriction in users' work-related access to personal data. 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.	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.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
B.7	System monitoring with an alarm feature has been established for the systems and databases used in the processing of personal data. This monitoring comprises: • User logins • Critical settings of systems and databases.	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. Checked by way of inspection of a sample of alarms that these were monitored, followed up on and that the data controllers were informed thereof as appropriate.	No exceptions noted.
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	Checked by way of inspection that formalised procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognised algorithm. Checked by way of inspection that technological encryption solutions have been available and active throughout the assurance period. Checked by way of inspection that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email. 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.	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.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests

B.9	Logging of the following matters has been established in systems, databases and networks:
	• Activities performed by system administrators and others holding special rights
	• Security incidents comprising:
	  ○ Changes in log set-ups, including disabling of logging
	  ○ Changes in users' system rights
	  ○ Failed attempts to log on to systems, databases or networks.
	Logon data are protected against manipulation and technical errors and are reviewed regularly.
		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.
		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.
		Checked by way of inspection that user activity data collected in logs are protected against manipulation or deletion.
		Checked by way of inspection of samples 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.
		Checked by way of inspection of samples of logging that documentation confirms the follow-up performed on activities carried out by system administrators and others holding special rights.
			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.	Data processor'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.	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. Checked by way of inspection of samples of development or test databases that personal data included therein are pseudonymised or anonymised. Checked by way of inspection of samples 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.	No exceptions noted.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	Checked by way of inspection that formalised procedures are in place for regularly testing technical measures, including for performing vulnerability scans and penetration tests. Checked by way of inspection of samples that documentation confirms regular testing of the technical measures established. Checked by way of inspection that any deviations or weaknesses in the technical measures have been responded to in a timely and satisfactory manner and communicated to the data controllers as appropriate.	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.	Data processor'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.	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. 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.	We have noted that two Domain Controller servers have not been patched aligned with approved procerus. We have received evidence after our test that these servers have been patched properly. No further exceptions 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.	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. 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. Checked by way of inspection of a sample of resigned or dismissed employees that their access to systems and databases was deactivated or removed in a timely manner. 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.	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.	Data processor'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.	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. 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.	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.	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. 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.	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.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
C.1	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. Assessments are made on a regular basis – and at least once a year – as to whether the information security policy should be updated.	Checked by way of inspection that an information security policy exists that Management has considered and approved within the past year. Checked by way of inspection of documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No exceptions noted.
C.2	Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.	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. Checked by way of inspection of a sample of data processing agreements that the requirements in these agreements are covered by the requirements of the information security policy for security measures and security of processing.	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.	Data processor'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.	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. 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. Checked by way of inspection of samples of employees appointed during the assurance period that documentation states that the screening has comprised: • References from former employers • Certificates of criminal record • Diplomas.	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.	Checked by way of inspection of employees appointed during the assurance period that the relevant employees have signed a confidentiality agreement. Checked by way of inspection of samples of employees appointed during the assurance period that the relevant employees have been introduced to: • The information security policy • Procedures for processing data and other relevant information.	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.	Data processor'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.	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. 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.	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.	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. 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.	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.	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. Inspected documentation stating that all employees who have either access to or process personal data have completed the awareness training provided.	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.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
D.1	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. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	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. Checked by way of inspection that procedures are up to date.	No exceptions noted.
D.2	The following specific requirements have been agreed with respect to the data processor's storage periods and deletion routines: • 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. • 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.	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. 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. 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.	No exceptions noted.
D.3	Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been: • Returned to the data controller and/or • Deleted if this is not in conflict with other legislation.	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. 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.	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.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
E.1	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. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	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. Checked by way of inspection that procedures are up to date. 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.	No exceptions noted.
E.2	Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.	Checked by way of inspection that the data processor has a complete and updated list of processing activities stating localities, countries or regions. 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.	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.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
F.1	Written procedures are in place which include requirements for the data processor when using subprocessors, including requirements for subprocessing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place for using subprocessors, including requirements for subprocessing agreements and instructions. Checked by way of inspection that procedures are up to date.	No exceptions noted.
F.2	The data processor only uses subprocessors to process personal data that have been specifically or generally approved by the data controller.	Checked by way of inspection that the data processor has a complete and updated list of subprocessors used. 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.	No exceptions noted.
F.3	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.	Checked by way of inspection that formalised procedures are in place for informing the data controller when changing the subprocessors used. Inspected documentation stating that the data controller was informed when changing the subprocessors used throughout the assurance period.	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.	Data processor'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.	Checked by way of inspection for existence of signed subprocessing agreements with subprocessors used, which are stated on the data processor's list. 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.	No exceptions noted.
F.5	The data processor has a list of approved subprocessors disclosing: • Name • Company registration no. • Address • Description of the processing.	Checked by way of inspection that the data processor has a complete and updated list of subprocessors used and approved. Checked by way of inspection that, as a minimum, the list includes the required details about each subprocessor.	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.	Data processor'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.	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. Checked by way of inspection of documentation that each subprocessor and the current processing activity at such processor are subjected to risk assessment. 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. 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.	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.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
G.1	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. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	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. Checked by way of inspection that procedures are up to date.	No exceptions noted.
G.2	The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.	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. 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.	No exceptions noted.
G.3	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.	Checked by way of inspection that formalised procedures are in place for ensuring a valid basis of transfer. Checked by way of inspection that procedures are up to date. 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.	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.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
H.1	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. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	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. Checked by way of inspection that procedures are up to date.	No exceptions noted.
H.2	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.	Checked by way of inspection that the procedures in place for assisting the data controller include detailed procedures for: • Handing out data • Correcting data • Deleting data • Restricting the processing of personal data • Providing information about the processing of personal data to data subjects. Checked by way of inspection of documentation that the systems and databases used support the performance of the relevant detailed procedures.	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.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
I.1	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. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	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. Checked by way of inspection that procedures are up to date.	No exceptions noted.
I.2	The data processor has established the following controls to identify any personal data breaches: • Awareness of employees • Monitoring of network traffic • Follow-up on logging of access to personal data.	Checked by way of inspection that the data processor provides awareness training to the employees in identifying any personal data breaches. 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. 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.	No exceptions noted.
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.	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. Made inquiries of the subprocessors as to whether they have identified any personal data breaches throughout the assurance period. 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.	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.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
I.4	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: • The nature of the personal data breach • Probable consequences of the personal data breach • Measures taken or proposed to be taken to respond to the personal data breach.	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: • Describing the nature of the personal data breach • Describing the probable consequences of the personal data breach • Describing measures taken or proposed to be taken to respond to the personal data breach. Checked by way of inspection of documentation that the procedures available support that measures are taken to respond to the personal data breach.	No exceptions noted.

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: 4ecdf2cc-e8cb-4f9e-bfb0-5e4b63b8ee2c
IP: 93.165.xxx.xxx
2025-02-03 20:06:04 UTC

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2025-02-03 20:19:00 UTC

Iraj Bastar
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
PwC-medunderskriver
Serienummer: 945792b8-522b-4f8c-9f2d-bc89647c3d96
IP: 83.136.xxx.xxx
2025-02-03 20:20:08 UTC