www.pwc.dk

Unit IT Holding 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 Controller

February 2025

Contents

1. Management's statement

Unit IT Holding A/S processes personal data on behalf of Data Controller in accordance with the data processing agreement.

The accompanying description has been prepared for Data Controller who has used Unit IT Holding A/S' operational and hosting services and who has 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.

Unit IT Holding A/S uses B4Restore A/S and Global Connect A/S as subprocessor for hosting activities and backup services. This report uses the carve-out method and does not comprise control objectives and re- lated controls that Subprocessors performs for Unit IT Holding A/S.

Some of the control objectives stated in our description in section 3 can only be achieved if the complementary controls at Data Controller 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.

Unit IT Holding A/S confirms that:

a) The accompanying description in section 3 fairly presents Unit IT Holding A/S' information security and measures regarding operational and hosting services that has 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 Unit IT Holding A/S' information security and measures regarding operational and hosting services was 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 Unit IT Holding A/S' information security and measures regarding operational and 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 Unit IT Holding A/S' information security and measures regarding operational and hosting services in 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 Unit IT Holding A/S' information security and measures regarding operational and 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 Unit IT Holding A/S' information security and measures regarding operational and 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.

Middelfart, 19 February 2025
Unit IT Holding A/S

Jess Julin Ibsen
CEO

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 Controller

To: Unit IT Holding A/S and Data Controller

Scope

We have been engaged to provide assurance about Unit IT Holding A/S's description in section 3 of Unit IT Holding A/S' operational and hosting services in accordance with the data processing agreement with Data Controller 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 Unit IT Holding 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 Unit IT Holding A/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").

Unit IT Holding A/S uses B4Restore A/S and Global Connect as a subservice supplier of datacenter hosting and backup services. This report uses the carve-out method and does not comprise control objectives and related controls that B4Restore A/S and Global Connect A/S performs for Unit IT Holding A/SUnit IT Holding A/SUnit IT Holding A/S.

Some of the control objectives stated in Unit IT Holding A/S' description in section 3 can only be achieved if the complementary controls at Data Controller are suitably designed and operating effectively with Unit IT Holding 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.

Unit IT Holding A/S's responsibilities

Unit IT Holding 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 Unit IT Holding A/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 operational and 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

Unit IT Holding 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 operational and 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 Unit IT Holding A/S' information security and measures regarding operational and 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 Unit IT Holding A/S' operation and 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, 19 February 2025
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

3. Description of processing

The purpose of the data processor's processing of personal data on behalf of the data controller is storing data in Unit IT's operations centers, so-called managed services, including ensuring stable operation, maximum uptime, and managing planned service windows of the managed services provided to the company's customers.

General description of Unit IT Holding A/S

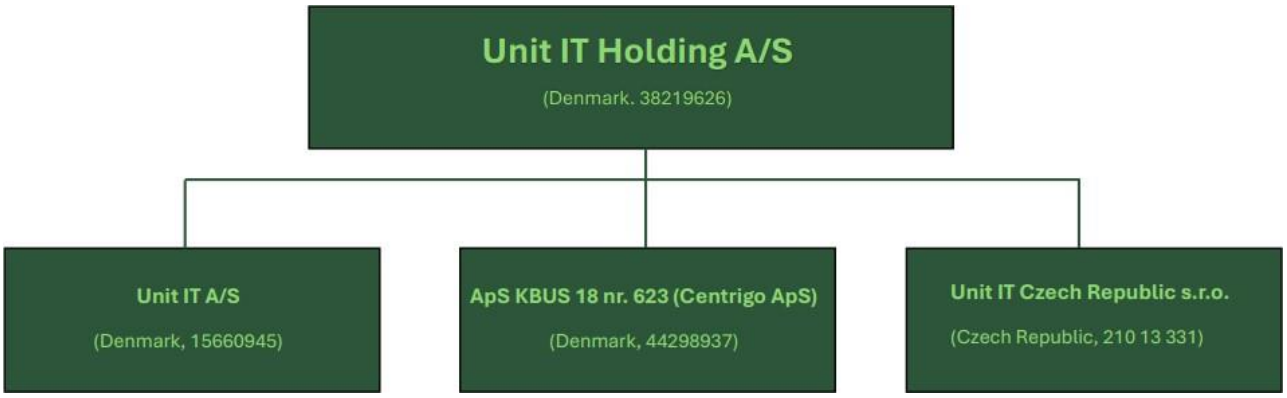
Unit IT Holding A/S (Unit IT) is a part of the USTC corporation in Middelfart. Unit IT is a managed services provider and provides a wide range of services that spans from infrastructure & cloud, managed services, Security, Cyber Defense Center, consulting, data and AI services to a wide range of public and private enterprises.

Unit IT currently has two data centres in Middelfart, from here, approx. 3,000 servers are monitored and operated. Furthermore, Unit IT utilizes multiple external data centres e.g. IBM, Microsoft Azure and Global Connect.

This description is intended to report on the general controls that Unit IT implements to support and safeguard its customers.

Unit IT is organized into functional business units, operating in a structured manner aligned with the guiding and normative requirements outlined in ISO31010, ISO27001, ISO27005 and ISO22301. This structural composition fosters an environment conducive to delivering and maintaining a consistently high level of service to Unit IT's customers. Unit IT places significant importance on achieving high service standards and ensuring customer satisfaction, recognizing these as critical elements in mitigating potential risks.

Unit IT has approximately 230 employees and is headed by Managing Director Jess Julin Ibsen, who reports to the USTC group.



- 1 March 2024: Unit IT Holding A/S acquired Global Connect Outsourcing Services (ApS KBUS 18 nr. 623), which has since been fully integrated into Unit IT Holding A/S.
- 1 April 2024: Unit IT Holding A/S established a new office in the Czech Republic (Unit IT Czech Republic s.r.o.), which also operates as an integrated part of the organization.

The entities Unit IT A/S, ApS KBUS 18, and Unit IT Czech Republic s.r.o. collectively constitute Unit IT Holding A/S.

Except for the organizational changes described above, there has been no major changes to procedures and internal controls during the period from 1. January to 31. December 2024.

Nature of processing

The data processor's processing of personal data on behalf of the data controller primarily concerns storage of data in Unit IT's operations centers, also known as managed services. This includes ensuring stable oper-

ation, maximum uptime, and managing planned service windows for the managed services that are delivered to Unit IT's customers.

The data processor's processing of personal data on behalf of the data controller primarily concerns hosting, storage and backup. Unit IT does not carry out any processing other than data storage (e.g. development activities). Unit IT does not access or modify the data unless explicitly requested by the data controller through the standardized support/change request process.

Personal data

The categories of data subjects whose personal data are processed by the data processor depend on the data that the data controller stores when using Unit IT's hosting services. All types of data are being processed according to the data processing agreements.

In accordance with the data processor's ISO 27001:2022 certification, a wide range of technical and organizational control measures have been implemented, cf. Article 32 of the Data Protection Act.

Risk assessment

Top management holds ultimate responsibility for Unit IT's information security and risk management. The core principle is that information security is grounded in the actual risks the company is exposed to.

Unit IT's utilizes 2 different risk methodologies. Initially ISO27001 risk assessments are based on the implementation guidelines in ISO31010 and ISO27005 subsequently following an Octave approach.

Secondly, a customized approach for assessing risks related to software vulnerabilities has been implemented across the organization. This method addresses specific risks that cannot be effectively managed using the previously mentioned methodologies, such as Octave and ISO 27001, in day-to-day operations. It leverages tailored impact assessments and mitigations to ensure comprehensive risk management.

Unit IT has a formal, management-approved process for risk management that results in action plans. These action plans are assigned and addressed in accordance with the risk treatment process.

The initial Octave risk analysis involves a hypothetical assessment of the consequence (extent) which may negatively affect Unit IT and the probability that a given incident manifests itself through the exploitation of vulnerabilities. The analysis is used to identify the potential risks where Unit IT should implement mitigating measures, and a plan is drawn up that can reduce the risk to an acceptable level.

Progress and deviations are regularly communicated to the Security Committee so that deviations and exceptions can be identified and addressed as part of management's review of risk management activities. Security validates results and the CISO reports to the Security Committee about metric changes in Security score, CMMI score as well as risk and BIA scale changes in relation to Risk.

All critical systems/information assets from ISO31010 BIA must be reviewed annually. Non-critical systems/information assets are assessed during implementation, as well as in the event of major changes in the organization, e.g. acquisitions, relocation of offices, changes in the technical infrastructure, or introduction of new or changed IT services which are estimated to affect Unit IT's business or ability to be in control of critical assets.

Control measures

Control objective A

Unit IT has established written procedures to ensure personal data is only processed when clear, written instructions are available. These procedures are regularly reviewed to determine whether updates are necessary, at least annually. The data processor will only process personal data as instructed by the data controller. Data processing agreements, which form the foundation for all data processing activities, are stored electronically in a central repository.

Control objective B

Unit IT has implemented robust controls to ensure consistent and structured user rights administration and access management. Access to systems follows the principle of least privilege, with users granted only the minimum access necessary for their roles. Elevations of access rights require formal management approval. Privileged accounts are created according to a strict process, incorporating the four-eyes principle (Segregation of Duties - SoD).

Access credentials, including usernames and passwords, adhere to strict policies for complexity and periodic rotation to reduce the risk of compromise. User accounts and permissions are reviewed regularly to ensure appropriateness, with unnecessary access revoked promptly.

Technical access controls are in place across all systems to prevent unauthorized or forceful login attempts. All system access activities are continuously monitored by a Security Information and Event Management (SIEM) solution, which generates alerts for abnormal events, directing them to the Cyber Defense Center (CDC) for immediate investigation and response.

Unit IT also employs comprehensive cryptographic controls to safeguard data in transit and at rest, tailored to the infrastructure's specific security needs and in compliance with regulatory and contractual obligations.

Secure Operations and Change Management

Unit IT has documented operational procedures to ensure secure and consistent system operations. These procedures cover managing contractual obligations, mitigating operational risks, and ensuring compliance with security standards. Key measures include:

- Change Management: All system changes undergo a rigorous approval process via the Change Advisory Board (CAB), including input from the customer or Unit IT, as applicable, to ensure changes align with security policies.
- Malware Protection: Systems are protected from malware and viruses through up-to-date protective measures and real-time scanning.
- Backup and Recovery: Regular backups are conducted, tested for reliability, and stored in secure, offsite locations.
- Vulnerability Monitoring: Systems and devices are proactively monitored for vulnerabilities, with findings integrated into the SIEM for centralized oversight and remediation planning.

Network and System Security

Unit IT employs multiple layers of protection for its information networks and processing facilities. Networks and associated equipment are strictly controlled, managed, and continuously monitored. Firewalls are configured to allow only necessary traffic, in line with the least privilege principle for IP and port access. Networking devices are regularly updated with security patches as recommended by manufacturers.

Periodic vulnerability scans of Unit IT systems identify and mitigate potential weaknesses. This emphasis on robust access management, secure operations, and proactive monitoring contributes to the resilience of Unit IT's information systems and networks.

Physical controls

Unit IT has implemented robust physical and organizational security measures to protect its hosting and housing facilities. Access is restricted to authorized personnel on a need-to-know, role-specific basis. Physical barriers, such as secure locks, biometric authentication, and CCTV surveillance, along with logical access controls, ensure comprehensive protection.

Environmental risks are mitigated with fire suppression systems, water detection sensors, and climate control mechanisms, all of which are regularly maintained. The facilities are designed with redundancy to ensure high availability and service continuity, incorporating backup power systems (UPS, generators) and redundant cooling systems. Surge protection mechanisms safeguard equipment from power fluctuations.

Surveillance systems, security personnel, and automated alerts provide 24/7 monitoring of the facilities, ensuring quick detection and response to any potential threats. Independent audits and assessments are conducted annually to ensure compliance with ISO27002:2022 and industry best practices.

Control objective C

Unit IT has established an Information Security Policy (ISP) that all employees must follow. This policy defines the responsibilities related to information security and governs the Information Security Management System (ISMS), ensuring it aligns with recognized industry standards and best practices, such as ISO 27001. The policy is reviewed at planned intervals to maintain its relevance and effectiveness.

All employees undergo mandatory training in information and cybersecurity. The training is periodically assessed, and results are closely monitored by management to ensure compliance with security protocols and to identify any gaps in knowledge.

The Acceptable Use Policy establishes clear guidelines for the appropriate use of company IT resources, including mobile devices, computers, and external media. Employees are required to adhere to these guidelines. This policy also governs the use of the company's network and applications, emphasizing secure and responsible behavior.

Access rights to information systems are granted strictly on a need-to-know basis, following the principle of least privilege. Role-based access controls ensure that employees only have access to the

Control objective D

Unit IT has implemented controls to ensure that upon the termination of processing services, the data exporter, at the choice of the data importer, will either delete all personal data processed on behalf of the data importer and provide certification of deletion, or return all personal data and delete any existing copies.

The data importer will certify the deletion of data to the data exporter. Until the data is either deleted or returned, the data importer remains responsible for ensuring compliance with these terms. In cases where local laws applicable to the data importer prohibit the deletion or return of the personal data, the data importer guarantees that it will continue to ensure compliance with these provisions, processing the data only to the extent and for the duration required by such local laws.

Control objective E

Unit IT has implemented procedures and processes for managing access to customer data. Access to customer systems, services, or configurations provisioned on platforms provided by Unit IT is governed by strict access controls, utilizing tiered access models and defined roles. Additionally, all sessions are logged and actively monitored.

All data processing by Unit IT occurs within the localities, countries, or regions that have been approved by the data controller.

Control objective F

Unit IT has implemented a process to oversee its sub-processors. This process includes a set of controls to ensure that Unit IT regularly evaluates the subservice supplier's compliance with agreed contractual obligations. These controls include, but are not limited to:

- Annual collection of ISAE or SOC reports from the subservice supplier's independent body, if applicable based on the criticality of the sub-supplier and sub-processor.
- Annual collection of the subservice supplier's ISO27001 certificate, if applicable based on the criticality of the sub-supplier and sub-processor.

Control objective G

Unit IT does not transfer personal data to third countries or international organizations.

Control objective H

Procedures and controls are in place to ensure that the data processor can assist the data controller in fulfilling requests related to the access, correction, deletion, or restriction of personal data processing by data subjects.

Unit IT will not act on any data subject request without first notifying and involving the data controller. Furthermore, no personal data will be disclosed to the data subject without prior written consent from the data controller, unless Unit IT is legally required to do so.

Control objective I

Unit IT has established procedures that include a requirement for the data processor to inform the data controller in the event of any personal data breaches.

Also refer to section 4 for a description of the specific control activities.

Complementary controls at the data controllers

As part of the service delivery, the data controller must implement and properly manage specific controls necessary to achieve the control objectives outlined in the description. These controls include, but are not limited to:

- Conducting risk assessments in accordance with Article 32 of the Regulation, and based on the findings, informing Unit IT about any additional technical or organizational measures intended to be implemented.
- Notifying Unit IT of any changes in risks or in the processing or categories of data that may impact the type of processing carried out on behalf of the data controller.
- Ensuring that adequate training and awareness programs are provided to users in the Data Controller's organization regarding procedures for handling personal data.
- Confirming that the implemented security measures are sufficient to ensure adequate protection of personal data processing
- Ensuring that the personal data provided to Unit IT is accurate and up to date.
- Verifying that access provisioning for personal data at the Data Controller is appropriate.

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 a sample of personal data processing operations that these are 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 a sample 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.	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 that, in a sample of alarms, these were 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 a sample of days 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 a sample of days 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 a sample of development or test databases that personal data included therein are pseudonymised or anonymised. 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.	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.	No 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 comprises, as relevant: • References from former employers • Certificates of criminal record • Diplomas	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 employees appointed during the assurance period that documentation states that the screening has comprised: • References from former employers • Certificates of criminal record • Diplomas	We have observed during our audit that there is a lack of verification and screening of employees in connection with employment. However, Unit IT has drawn up a procedure for the same, which is why we expect that the observation will be removed for the next period. No further 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 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.	We have observed that one user in the inspected sample do not have a signed contract/NDA. No further 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.	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. Checked by way of inspection of documentation that there has been a timely follow-up on logging access to personal data, including monitoring repeated attempts to access.	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.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. 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.	No exceptions noted.
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."

Jess Julin Ibsen
Kunde
Serienummer: c51d4162-810e-4a38-8c1b-2deada7381a0
IP: 62.243.xxx.xxx
2025-02-19 08:05:21 UTC

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2025-02-19 08:19:14 UTC