www.pwc.dk

EG Danmark A/S

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 15 June 2024 to 31 December 2024 pursuant to data processing agreements in relation to EG Danmark A/S's development and operating services for Mainmanager

August 2025

pwc

Contents

1. Management's statement

EG Danmark A/S processes personal data on behalf of customers (data controllers) in accordance with data processing agreements in relation to development and operating services.

The accompanying description has been prepared for customers who have used EG Danmark A/S's development and operating 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.

EG Danmark A/S uses team.blue Denmark A/S as subprocessors of housing, network, virtual server and storage services. This report uses the carve-out method and does not comprise control objectives and related controls that team.blue Denmark A/S performs for EG Danmark A/S.

EG Danmark A/S uses B4Restore A/S as a subprocessor of backup services. This report uses the carve-out method and does not comprise control objectives and related controls that B4Restore A/S performs for EG Danmark 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.

EG Danmark A/S confirms that:

a) The accompanying description in section 3 fairly presents EG Danmark A/S's development and operating services that have processed personal data for data controllers subject to the data protection rules throughout the period from 15 June 2024 to 31 December 2024. The criteria used in making this statement were that the accompanying description:

   (i) Presents how EG Danmark A/S's development and operating 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 EG Danmark A/S's development and operating 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 development and operating services for the processing of personal data in the period from 15 June 2024 to 31 December 2024;

(iii) Does not omit or distort information relevant to the scope of EG Danmark A/S's described development and operating services 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 development and operating 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 15 June 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 15 June 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.

Ballerup, 19. august 2025
EG Danmark A/S

Signed by:
Guðrún Rós Jónsdóttir
26A8191EF41E420...

Guðrún Rós Jónsdóttir
Director

pwc

2. Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 15 June 2024 to 31 December 2024 pursuant to data processing agreements in relation to EG Danmark A/S's development and operating services for Mainmanager

To: EG Danmark A/S and EG Danmark A/S's customers

Scope

We have been engaged to provide assurance about EG Danmark A/S's description in section 3 of EG Danmark A/S's development and operating services in accordance with data processing agreements with data controllers throughout the period from 15 June 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 EG Danmark 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 EG Danmark 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").

EG Danmark A/S uses team.blue Denmark A/S as subprocessors of housing, network, virtual server and storage services. This report uses the carve-out method and does not comprise control objectives and related controls that team.blue Denmark A/S performs for EG Danmark A/S.

EG Danmark A/S uses B4Restore A/S as a subprocessor of backup services. This report uses the carve-out method and does not comprise control objectives and related controls that B4Restore A/S performs for EG Danmark A/S.

Some of the control objectives stated in EG Danmark 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 EG Danmark 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.

EG Danmark A/S's responsibilities

EG Danmark 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 EG Danmark 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 development and operating 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

EG Danmark 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 EG Danmark A/S's development and operating 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 EG Danmark A/S's development and operating services as designed and implemented throughout the period from 15 June 2024 to 31 December 2024;

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 15 June 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 15 June 2024 to 31 December 2024.

Description of test of controls

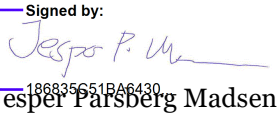
The specific controls tested and the nature, timing and results of those tests are listed in section 4.

pwc

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 EG Danmark A/S's development and operating 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. august 2025
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Signed by:

186835G51BA6430

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

3. Description of processing

Introduction and scope

This system description concerns the IT general controls related to application development and hosting activities at EG Danmark A/S, which is owned by the private equity fund Francisco Partners. Standard IT operations and hosting activities are provided by EG CloudOps, and application development is handled by the individual business units, which in this report are referred to as EG.

As far as application development is concerned, EG works according to the same procedures and methods on all development tasks.

EG uses team.blue Denmark A/S as subservice suppliers of physical security in data centres where customer operations are performed. team.blue Denmark A/S are e.g. responsible for physical security, hardware, network, backup, hypervisor and storage.

EG Danmark A/S uses B4Restore A/S as a subprocessor of backup services.

This report uses the carve-out method and does not comprise controls performed by subservice suppliers. For 2024, these controls are covered by auditor's reports received from the subservice suppliers.

EG handles operation and monitoring in connection with IT operations and hosting activities and is responsible for ensuring the implementation and operation of control systems to prevent and detect errors, including intentional errors, in order to comply with contracts and best practice.

This description is limited to general standards of administration as described in EG's standard contract. Specific matters related to individual customer contracts are not covered.

Based on the above delimitation and the system description specified below, EG assesses that we have maintained effective controls in all material matters. EG is aware of the continuous development in the area and continuously works to improve the controls.

EG specialises in building and delivering industry-specific vertical software. This report covers EG's deliverables under customer contracts with a view to EG's compliance with its obligations as a data processor under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 July 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (hereinafter referred to as GDPR).

The GDPR work is divided into two focus areas: the internal area which concerns all internal processes in which we as a company deal with personal data (e.g. HR, IT, marketing and finance) and the customer-facing area – covered by this report – which concerns all areas in which we interact with our customers and potentially could come into contact with personal data.

Description of services covered by the report

The services provided by EG are tailored to several different types of customers. The conditions for the individual customers are specified in contracts; each business area is based on standard contracts which may contain individual adjustments and options. The following areas cover the services offered by EG:

- Hosting
- Application development
- Consulting
- Implementation

EG delivers the following solutions and modules to the customers:

EG MainManager

Control environment

Management structure

Compliance with the requirements in relation to IT security follows the organisation established in relation to the management of information security as described below.

At EG, the organisational set-up and management are based on a structure by function where the manager of the individual department has staff responsibilities. The responsibility for security of the individual processes lies with the individual(s) responsible and the performing individual(s), respectively. The manager responsible has the responsibility of ensuring that the process is followed and documented by the performing employees.

Organisation of information security (control objective B)

The overall responsibility for IT security at EG and associated companies lies with the IT security committee (EG Security Committee) which deals with all major relevant IT security matters of a fundamental nature. The IT security committee is represented by employees from top management, division managers, the Vice President of IT, CIO, CISO and the General Counsel of Group Legal & Compliance. The IT security committee reports directly to the Executive Board of EG.

The committee is normative, and based on the adopted IT security policy it lays down the principles and guidelines that are to ensure objectives are met. Security incidents, status and security weaknesses are reported to the IT security committee which initiates any further action. Like all other employees, members of the IT security committee regularly participate in relevant awareness training within IT security. The IT security is executed through internal strategy, policies, standards, procedures and guidelines.

The operational responsibility for the management of the cyber and information security in EG is placed on the central Cyber and Information Security Team headed by the Chief Information Security Officer (CISO). This team defines security policies, requirements and guidance for the whole EG organization, coordinates implementation of security measures across the organization, as well as operates centrally delivered security processes. The Cyber and Information Security Team is responsible for ensuring that EG employees are kept up to date with the security regulations.

Particular responsibility for following security policies, requirements and guidance and implementation of required security measures lies on the organizational units that develop and maintain EG systems: EG IT, CloudOps, DevOps and individual Business Units. Those units nominate Security Coordinators who are liaisons with the Cyber and Information Security Team and who coordinate security activities in their units. They also nominate Local Security Incident Coordinators responsible for security incident management in these units.

All EG personnel, including employees, as well as third parties with access to EG systems, have a responsibility to protect EG's information against unauthorized access, alteration, destruction and theft. Therefore, all employees are made familiar to the Security Handbook and are required to complete the required security trainings or assignments. Depending on the role in the organization, employees are also communicated about specific security policies and procedures.

EG established and maintains a Cyber and Information Security Management System (C&ISMS) with a goal to ensure an adequately high level of security, compliant with relevant legal and other external requirements. The C&ISMS takes a risk-based approach in ensuring the adequate security level. Security objectives, security strategy, as well as decisions as to which security measures to apply take into account the impact and probability of risks addressed. Performance and effectiveness of the C&ISMS is monitored and evaluated, including effectiveness of key processes, status of actions to achieve security objectives or risk treatment plans, effectiveness of security measures, as well as risk and security levels. A combination of measures may be applied such as: KPI measurement, audits, penetrations tests, security scans, risk assessments and management reviews. All identified nonconformities, weaknesses and improvement possibilities result in preparation of actionable plans to continually improve the suitability, adequacy and effectiveness of the C&ISMS.

GDPR Committee

The overall responsibility for data protection matters of a fundamental nature lies with EG's GDPR Committee.

The GDPR Committee (GDPR Committee) is a normative committee for EG's strategy and risks in relation to GDPR-related topics. The committee supports and ensures efficient business and best practice within data protection across EG Danmark A/S and associated companies.

The chairman of the GDPR committee is appointed by the CFO and elected from among the committee members. In addition, a secretary of the committee is elected from among the employees of Group Legal & Compliance.

The GDPR Committee lays down applicable data protection principles and guidelines in accordance with the GDPR and other national data protection legislation. It takes GDPR initiatives, facilitates relevant awareness and training and ensures an optimal audit process (ISAE 3402 and ISAE 3000).

Education and training

When policies, guidelines and procedures (standard operating procedures) are updated, this is communicated to all employees. Policies and procedures are available in EG's ISMS system in which employees can always find information. If an employee becomes aware of errors and defects, he or she must inform the relevant contact person or department listed in the relevant policy or procedure.

Compliance with instructions from the data controller (control objective A)

EG has established a number of GDPR policies and procedures that employees have received and are trained to comply with. These e.g. include:

- GDPR Handbook for Employees
- Code of Conduct Employees
- Security Incident Management Policy
- Whistleblower Scheme
- Email Policy
- Privacy & Cookie Policy
- GDPR-related procedures (SOP).

EG processes personal data in accordance with the customer's instructions. EG does not process personal data without having entered into a data processing agreement with the data controller (the customer). EG has a standard data processing agreement which is updated at least once a year by Group Legal & Compliance. EG's standard data processing agreement is based on the Danish Data Protection Agency's template. Each solution area must draw up a data processing agreement based on EG's standard data processing agreement containing defined requirements for the processing of personal data, including:

- Purpose of processing activity/activities

- Categories of personal data
- Sub-processors
- Transfer to a third country.

Sub-processors to carry out specific processing activities on behalf of the customer are only used after the customer has approved the use of the sub-processor. In the data processing agreement, EG has ensured that all sub-processors comply with the same data protection obligations as those defined in the data processing agreement between EG and the customer.

For each solution area and cross-disciplinary process – cf. previous sections – appropriate technical and organisational controls have been established in these areas.

A continuous assessment is carried out as to whether EG still has the necessary appropriate technical and organisational security measures in place to continue to deliver the solution and service in question to the customer.

Technical and organisational measures (control objectives B and C)

For information on technical and organisational controls, please refer to the prepared ISAE 3402 reports. These include areas such as:

- Human resource security
- Security incident management
- External parties and supplier relationships
- Physical security
- Operating procedure
- Monitoring and logging
- Segregation of duties
- Encryption
- Backup and restore
- Error correction and support
- Access control
- Acquisition, development and maintenance of systems
- Acquisition, development and maintenance of applications
- Disaster recovery plans.

Development, testing and maintenance:

As a general rule, personal data used for development, testing or similar activity is in pseudonymised or anonymised form. It is used only to act in the interests of the customer according to agreement and on the customer's behalf. In certain cases, it may be necessary to test on real data, and personal data will then be transferred from production to test environment. In such cases, approval must be obtained from the customer.

Organisation of data protection and the data protection officer:

EG has not appointed a data protection officer as the primary activity of the group's core business does not involve the processing of personal data. Instead, EG has a Data Protection Office, which is anchored in EG's legal department, Group Legal & Compliance. The department carries out general legal tasks within IT, the GDPR and compliance.

The data processor assists the data controller:

To the extent that EG is responsible for processing personal data on behalf of and on instructions from the data controller, EG assists the data controller in ensuring compliance with:

- the responsibility to implement appropriate technical and organisational security measures to ensure a level adapted to the risks associated with the processing

- the responsibility to report a personal data breach to the controlling authority (the Danish Data Protection Agency) without undue delay and, where feasible, no later than 72 hours after having become aware of the security breach unless the personal data breach is unlikely to result in a risk to the rights and the freedoms of natural persons

- the responsibility to notify the data subject(s) about the personal data breach without undue delay when a personal data breach is likely to involve a high risk to the rights and freedoms of natural persons

- the responsibility to carry out a data protection impact assessment if a type of processing is likely to involve a high risk to the rights and freedoms of natural persons

- the responsibility to confer with the controlling authority (the Danish Data Protection Agency) before processing if an impact assessment regarding data protection shows that the processing will result in a high risk because of the arrangements made by the data controller to minimise the risk.

Erasure procedure (control objective D)

EG has written procedures for erasure of personal data in accordance with the data processing agreement concluded with the customer.

Special requirements for erasure of personal data, including deletion routines, follow specifically from the data processing agreement concluded with the customer.

The system has automation that anonymises all personal data fields for registered persons in the system within 5 years after the person is has stopped using the system and has end date.

Upon termination of the processing of personal data for the data controller, EG will either return the personal data to the data controller and/or erase the personal data, providing this does not conflict with other legislation. The specific procedure for termination of processing of personal data is agreed under instructions from the customer in accordance with the data processing agreement with the customer.

Storage procedure (control objective E)

EG has written procedures for storage of personal data in accordance with the data processing agreement concluded with the customer.

Special requirements for storage and erasure of personal data, including storage periods, are specifically set out in the data processing agreement concluded with the customer.

An overview of processing activities and indication of locations, countries and regions for EG as a data processor and EG's sub-processors is included in the data processing agreement concluded with the customer.

Sub-processors (control objective F)

EG has concluded data processing agreements with all its sub-processors to ensure the same data protection obligations as those provided in the data processing agreement with the customer. EG only uses sub-processors for the processing of personal data upon specific or general approval by the data controller.

EG maintains an overview of all approved sub-processors, comprising, as a minimum, the individual sub-processor's name, company registration no. or similar, address and description of processing activity.

New sub-processors of EG

All new sub-processors of EG are assessed and approved by EG's Vendor Approval Board (VAB).

VAB consists of Vice President of Procurement, CTO and General Counsel from Group Legal & Compliance.

In addition, a secretary of VAB is elected from among the employees of Group Legal & Compliance.

VAB ensures a common approval process for all sub-processors and that the sub-processors comply with EG's requirements regarding technology, security, compliance and data protection.

Supervision of sub-processors

EG carries out supervision of all sub-processors at least once a year based on a risk assessment. Supervision of sub-processors is carried out centrally in EG's legal department, Group Legal & Compliance. The supervision ensures and documents the sub-processors used for the service that EG provides to the customer in relation to:

- GDPR compliance, including ensuring adequate protection of data subjects' rights in accordance with the GDPR if personal data is processed
- Compliance with equivalent technical security measures as specified in the data processing agreement with the customer
- Compliance with equivalent organisational security measures as specified in the data processing agreement with the customer.

All final approvals of supervision reports on sub-processors are made by VAB.

Transfer of data to third countries or international organisations (control objective G)

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 data processing agreement with the data controller by using a valid basis of transfer.

The rights of the data subject (control objective H)

In consideration of the nature of the processing, EG assists the data controller – as far as possible and by means of appropriate technical and organisational measures – in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights under the GDPR.

EG has a procedure for handling and documenting enquiries from the data controllers in relation to assisting with handling the rights of the data subjects (access, erasure, rectification, etc.).

The specific procedure and controls for handling and documenting assistance to the data controller are set out in the data processing agreement concluded between EG and the customer.

Procedure for handling security breaches (control objective I)

In case of any (potential) personal data breaches, EG – as a data processor – must notify the data controller in accordance with the data processing agreement after having become aware of a personal data breach at EG or at EG's sub-processor.

As a data processor, EG assists the data controller with the reporting of data breaches to the Danish Data Protection Agency.

Complementary controls at the data controllers

As part of the delivery of services, the data controller must implement certain controls that are important to achieve the control objectives specified in the description. This includes:

- Consideration of consequences in relation to personal data protection when changes are made to existing solutions (privacy by design and privacy by default) and submission of a request for change to EG to the extent relevant
- Consideration of / testing of new versions of solutions in connection with implementation (change management)
- Set-up and administration of own users of the solution in the production environment (identity and access management)
- Set-up and administration of users from EG who have access to the customer's environment (identity and access management).

Improvements

In 2024, EG has taken the following measures to improve the level of security and data protection:

Month	Measures
August 2024	EG Danmark A/S implemented new governance, risk management and compliance system ZenGRC, with the following goals: • Improved Security Risk Management process (including NIS2 aspects of impact on society, country and markets) • Improved Vendor Risk Management EG Denmark A/S implemented a security tool for verification and management of security posture of its public Cloud Environments

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.	We have noted that no formalised procedure is in place and that the review has been documented. We have noted that this has been remediated in 2025. No further 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, e.g. in the event of a compromise.	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 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. TLS encryption in connection with the transmission of emails complies with the Danish Data Protection Agency's requirements in this area.	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: o Changes in log set-ups, including disabling of logging o Changes in users' system rights o Failed attempts to log on to systems, databases or networks. Log information is protected against manipulation and technical errors and is 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 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 logging that documentation confirms the follow-up performed on activities carried 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 and test databases that personal data included therein are pseudonymised or anonymised. Checked by way of inspection of a sample of development and 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. Significant vulnerabilities are remedied within a specified and acceptable time frame.	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 a sample 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. Security patches are installed according to the vendor's recommendations and release cycle.	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 and at least every six months, 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.	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 or a secured jump host solution.	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.	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 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	The data processor has implemented a process for termination of employment to ensure that users' rights are deactivated or terminated, including that assets are returned.	Inspected procedures ensuring that terminated 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 termination, 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	Any agreed specific requirements for the data processor's storage periods and deletion routines in accordance with the concluded data processing agreements are followed.	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 sub-processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.

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 sub-processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.

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 sub-processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.

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 sub-processor 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 sub-processing 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.

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 in-formed the data controller without undue delay and in accordance with the data processing agreement 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 in accordance with the data processing agreements after the data processor became aware of the personal data breach.	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. Checked by way of inspection of documentation that, when a personal data breach occurred, measures were taken to respond to such breach.	No exceptions noted.