EG Danmark A/S and EG Norge AS

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 January 2025 to 31 December 2025 pursuant to the data processing agreement in relation to EG Danmark A/S and EG Norge AS's development and operating services regarding EG Healthcare

July 2026

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

Contents

1. Management's assertion 3
2. Independent auditor's report 5
3. Description of processing 8
4. Control objectives, control activity, tests and test results 16

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

1. Management's assertion

EG Danmark A/S and EG Norge AS (EG) processes personal data on behalf of customers (data controllers) in accordance with the data processing agreement in relation to EG's development and operating services regarding EG Healthcare.

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

Microsoft Ireland Operations Ltd and team.blue Denmark Aps are subprocessors that provide hosting and backup services to EG. This report uses the carve-out method, and the description in section 3 includes only the control objectives and related controls of EG and excludes the control objectives and related controls of Microsoft Ireland Operations Ltd and team.blue Denmark Aps. Our evaluation did not extend to controls of Microsoft Ireland Operations Ltd and team.blue Denmark Aps.

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

EG confirms that:

a) The accompanying description in section 3 fairly presents information security and measures in relation to EG's development and operating services regarding EG Healthcare that have processed personal data for data controllers subject to the data protection rules throughout the period from 1 January 2025 to 31 December 2025. The criteria used in making this statement were that the accompanying description:

   (i) Presents how information security and measures in relation to EG's development and operating services regarding EG Healthcare 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

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

- Controls that we, in reference to the scope of EG's development and operating services regarding EG Healthcare, have assumed would be implemented by data controllers and which, if necessary in order to achieve the control objectives stated in the description, are identified in the description

- Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data

(ii) Includes relevant details of changes to the data processor's development and operating services regarding EG Healthcare for processing personal data in the period from 1 January 2025 to 31 December 2025

(iii) Does not omit or distort information relevant to the scope of the development and operating services regarding EG Healthcare being described for the processing of personal data, while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the development and operating services regarding EG Healthcare that each individual data controller may consider important in its own particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 January 2025 to 31 December 2025. The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 January 2025 to 31 December 2025.

c) Appropriate technical and organisational measures were established and maintained to comply with the agreements with the data controllers, sound data processing practices and relevant requirements for data processors in accordance with the data protection rules.

Aarhus, 2 July 2026
EG Danmark A/S and EG Norge AS

Laila Aarseth
Vice President

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

2. Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 January 2025 to 31 December 2025 pursuant to the data processing agreement in relation to EG's development and operating services regarding EG Healthcare

To: EG Danmark A/S and EG Norge AS (EG) and data controllers

Scope

We have been engaged to report on EG's description in section 3 of its development and operating services regarding EG Healthcare in accordance with the data processing agreement with data controllers throughout the period from 1 January 2025 to 31 December 2025 (the description) and on the suitability of the design and operating effectiveness of controls related to the control objectives stated in the description.

Our report covers whether EG 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'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").

Microsoft Ireland Operations Ltd and team.blue Denmark Aps are subprocessors that provide hosting and backup services to EG. This report uses the carve-out method, and the description in section 3 includes only the controls objectives and related controls of EG and excludes the control objectives and related controls of Microsoft Ireland Operations Ltd and team.blue Denmark Aps. Our examination did not extend to controls of Microsoft Ireland Operations Ltd and team.blue Denmark Aps.

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

We express reasonable assurance in our conclusion.

EG's responsibilities

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

Auditor's independence and quality control

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

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

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

Auditor's responsibilities

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

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

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

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

Inherent limitations

EG'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's development and operating services regarding EG Healthcare that the individual data controller may consider important in its own particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect all personal data breaches. Also, the projection to future periods of any evaluation of the fairness of the presentation of the description, or opinions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

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

a) The description fairly presents the development and operating services regarding EG Healthcare as designed and implemented throughout the period from 1 January 2025 to 31 December 2025

b) The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls operated effectively throughout the period from 1 January 2025 to 31 December 2025, and if data controllers applied the complementary controls referred to in section 3

c) The controls tested, which together with the complementary controls at data controllers referred to in section 3, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 January 2025 to 31 December 2025.

Description of test of controls

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

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

Intended users and purpose

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

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

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

Aarhus, 2 July 2026
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

3. Description of processing

3.1. Introduction and scope

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 April 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.

3.2. Description of services covered by the report

The services provided by EG are tailored to several different types of customers. The terms for each customer are specified in contracts in which each business area is based on standard contracts, which may include individual adjustments and options.

The services offered by EG and covered by this report are the following:

- Providing applications in Software-as-a-Service model
- Providing applications in a Managed Service model in which the applications and the underlying infrastructure are managed by EG
- Providing applications (sale of licences) that subsequently are hosted and managed by EG's customers.

In order to ensure an adequate level of security irrespective of the model in which a particular application is provided, EG applies a common framework of controls described further in this document, focusing on application development as well as maintenance of applications and underlying infrastructure. As part of this framework, EG 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.

EG uses Microsoft Ireland Operations Ltd and team.blue Denmark A/S as subservice suppliers significant to the description and understanding of the scope of this report. Microsoft Ireland Operations Ltd and team.blue Denmark A/S provide hosting services, including data centre, hardware, storage and backup (up to the level of virtualisation platform). Microsoft Ireland Operations Ltd and team.blue Denmark A/S provide additional backup solutions and off-site storage. The controls applied by these service providers are not subject of this report. EG is strictly monitoring the level of security ensured by these providers and for 2025 obtained the audit reports from these suppliers.

3.3. Control environment

3.3.1. 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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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

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

- GDPR Handbook for Employees
- Security Incident Management Policy
- Code of Conduct Employees
- Whistleblower Scheme
- Email 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.

3.3.3. Organisation of information security (control objective B)

EG Security Committee

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 organisation, coordinates implementation of security measures across the organisation and 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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

Particular responsibility for following security policies, requirements and guidance and implementation of required security measures lies on the organisational units that develop and maintain EG systems: EG IT, CloudOps, DevOps and individual business units. Those units nominate security coordinators who act as liaison to 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.

EG has 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 and 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.

Compliance Committee

The Compliance Committee is responsible for the oversight of data protection and compliance matters of fundamental importance within EG. The committee is normative and has a cross-divisional function, integrating legal, technical, and business perspectives to ensure that EG comply with all applicable legislation, including the General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NIS2).

The committee's mandate includes the identification, assessment and mitigation of regulatory, legal and reputational risks arising from these and other relevant legal frameworks. The committee is authorised to make binding decisions, initiate necessary actions and allocate resources to ensure that EG's compliance obligations are fulfilled. Other areas addressed in the committee are GDPR initiatives, relevant awareness campaigns and training and ensure an optimal audit process (ISAE 3402 and ISAE 3000).

The committee is composed of the CFO, all divisional vice presidents (EVPs), representatives from the CTO and internal IT, the general counsel from Group Legal & Compliance and a member of Group Legal & Compliance. The committee reports to the Audit Committee from a corporate governance perspective. Meetings require a quorum of three members to make decisions. 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.

Education and training

All EG personnel – including employees and third parties with access to EG systems – are required to comply with data protection legislation, such as the General Data Protection Regulation (GDPR), and other applicable laws in their everyday work. In addition to statutory obligations, personnel must adhere to EG's internal policies and procedures, which include the GDPR Employee Handbook and the Code of Conduct. All EG personnel also have a responsibility to protect EG's information against unauthorised access, alteration, destruction and theft. To support this, all employees are made familiar with the Security Handbook and are required to complete mandatory security and compliance trainings or assignments.

Relevant awareness training on data protection, cyber information security and compliance requirements is provided on an annual basis, and personnel are required to participate in such training. Depending on their role in the organisation, employees are also informed about specific security and compliance policies and procedures relevant to their responsibilities.

This comprehensive approach ensures that EG's information is safeguarded and that all activities are conducted in accordance with both legal and internal requirements.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

3.3.4. 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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

3.3.5. 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.

Specific requirements regarding the erasure of personal data – including deletion routines – are determined by the data processing agreement entered into with each customer.

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.

3.3.6. 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 with the customer.

3.3.7. 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

EG has entered into data processing agreements with all sub-processors to ensure the same data protection obligations as those stipulated in the data processing agreement with the customer. EG only uses sub-processors for the processing of personal data with specific or general approval from the data controller.

EG maintains a register of all approved sub-processors, which includes, as a minimum, the name, company registration number (CVR) or similar, address and a description of the processing activity for each sub-processor.

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 Procurement. 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.

Risk-based supervision and audit

EG conducts an annual risk-based audit of all sub-processors. The supervision of sub-processors is carried out centrally in 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

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

- Compliance with equivalent organisational security measures as specified in the data processing agreement with the customer.

All audit responses and supporting documentation are reviewed by Group Legal & Compliance, and, if necessary, in collaboration with the relevant business unit. Supplementary questions or follow-up meetings may be conducted based on findings.

The audit process and results are documented and archived, and the completion is logged in C&ISMS. Final approval of audit reports is made by VAB and reported to the Compliance Committee. Summary reports can be provided to customers upon request.

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

EG only transfers personal data to third countries or international organisations in accordance with the data processing agreement with the data controller and applicable data protection legislation.

EG has established a comprehensive procedure to govern transfer of personal data to third countries or international organisations. EG's policies and procedures regarding third-country transfer applies to all EG staff, consultants and contracting staff.

The key steps and requirements are as follows:

- Before any transfer, EG verifies that a valid legal basis for the transfer exists (such as an adequacy decision, standard contractual clauses or other recognised mechanisms).

- Where required, EG conducts a transfer impact assessment to evaluate risks and determine if supplementary safeguards are necessary to ensure an adequate level of data protection equivalent to that of the EU/EEA.

- All steps and decisions related to third-country transfers are documented and subject to review by Group Legal & Compliance.

- EG regularly reviews and updates its procedures to ensure ongoing compliance with legal requirements for international data transfers.

3.3.9. 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 inquiries 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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

3.3.10. Procedure for handling security breaches (control objective I)

All security incidents are handled according to the established Security Incident Management Policy and procedures. If an employee becomes aware of a security incident, he or she must inform the appointed security incident manager, who is responsible for ensuring a quick, effective and timely response to information security incidents.

In the event of a security incident, the affected customers are notified as soon as possible, and steps are taken to secure data and systems. If agreed with the customer, a root cause analysis report is drawn up to ensure, as far as possible, that the incident cannot occur again.

All material security incidents are reported to Management.

In case of 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.

3.4. 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).

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

3.5. Improvements

In 2025, EG has taken the following measures to improve the level of security and data protection:

Month	Measures

November 2025	**In 2025, EG strengthened its position in cyber security and data protection through a range of strategic and operational initiatives.**
	
	• Our governance structure was reinforced through our cyber and information security framework, ensuring alignment with applicable requirements such as the CIS Controls, NIS2, the AI Act and GDPR.
	
	• We implemented key technical and organisational improvements, including:
	  ○ Expanded application security testing and enhanced vulnerability management capabilities
	  ○ Improved cloud security governance
	  ○ Expanded asset management through integrations with a central CMDB
	  ○ Further strengthened third-party risk management through new classification and assessment criteria as well as internal tools.
	
	Infrastructure and application security were enhanced through stricter data protection and security standards, automated vulnerability scanning, and an expanded penetration testing programme for applications and infrastructure.
	
	Data protection measures were updated and strengthened through comprehensive data classification, encryption standards, and updated testing of incident reporting processes to support new legislation such as NIS2.
	
	EG further invested in awareness training to raise employee security awareness and in continuous compliance monitoring to embed a culture of resilience and regulatory readiness across the organisation.
	
	EG implemented and rolled out guidelines for generative and agentic AI and MCP server governance, including approval workflows and integration patterns. EG has:
	
	• established formal working procedures to define and govern the secure adoption of AI across products and internal processes
	
	• introduced AI-assisted tools that connect vulnerability data to developers' workflows, and launched an AI-based threat modelling tool to accelerate consistent documentation and risk assessments
	
	Finally, EG revised the system descriptions in the audit statements to reflect new applicable legislation and to incorporate the relevant organisational changes resulting from these legal updates.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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 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. 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 personal data through the internet are protected by strong 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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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.
	Log 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 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 out by system administrators and others holding special rights.
			No exceptions noted.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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 XX 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. 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 samples that regular testing of the technical measures established is documented. Checked by way of inspection that any deviations or weaknesses in the technical measures have been attended to in a timely and satisfactory manner and communicated to the data controllers as appropriate.	No exceptions noted.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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 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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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 therein are covered by the requirements of the information security policy for security measures and security of processing.	No exceptions noted.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG'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 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 agreement after the data processor became aware of the personal data breach.	No exceptions noted.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

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.	EG's control activity	Tests performed by PwC	Result of PwC's tests
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency. These procedures must contain instructions on descriptions of: • The nature of the personal data breach • Probable consequences of the personal data breach • Measures taken or proposed to be taken to respond to the personal data breach.	Checked by way of inspection that the procedures in place for informing the data controllers in the event of any personal data breach include detailed instructions for: • Describing the nature of the personal data breach • Describing the probable consequences of the personal data breach • Describing measures taken or proposed to be taken to respond to the personal data breach. Checked by way of inspection of documentation that the procedures available support that measures are taken to respond to the personal data breach.	No exceptions noted.

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

PENNEO

The signatures in this document are legally binding. The document is signed using Penneo™ secure digital signature. The identity of the signers has been recorded, and are listed below.

"By my signature I confirm all dates and content in this document."

Laila Aarseth
Kunde
On behalf of: EG Danmark A/S and EG Norge AS
Serial number: bankid.no no_bankid:9578-5994-4-461424
IP: 89.8.xxx.xxx
2026-07-02 10:24:17 UTC

QES

bankID

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
On behalf of: PricewaterhouseCoopers Statsautoriseret…
Serial number: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2026-07-02 10:43:57 UTC

MitID

Penneo document key: 07AG1-HAP7H-JE8BN-AN94G-MNN1Y-L70B7

This document is digitally signed using **Penneo.com**. The signed data are validated by the computed hash value of the original document. All cryptographic evidence is embedded within this PDF for future validation.

The document is sealed with a Qualified Electronic Seal. For more information about Penneo's Qualified Trust Services, visit **https://eutl.penneo.com**.

How to verify the integrity of this document
When you open the document in Adobe Reader, you should see that the document is certified by **Penneo A/S**. This proves that the contents of the document have not been modified since the time of signing. Evidence of the individual signers' digital signatures is attached to the document.

You can verify the cryptographic evidence using the Penneo validator, **https://penneo.com/validator**, or other signature validation tools.