Cloud Factory A/S

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 23 May 2025 to 31 May 2026 pursuant to the data processing agreement with data controllers

June 2026

Penneo dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

Contents

Penneo dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

1. Management's assertion

Cloud Factory A/S (Cloud Factory) processes personal data on behalf of its customers (data controllers) in accordance with the data processing agreement governing the use of Cloud Factory's license management platform.

The accompanying description has been prepared for data controllers who have used Cloud Factory's license management platform 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.

Netic A/S is a subprocessor that provides housing of the primary and secondary data centres to Cloud Factory, and Intercom R&D Unlimited Company, Atlassian Pty Ltd, Autho Inc. and Functional Software Inc. are subprocessors that provide services in the license management platform, ticket system, multifactor authentication and monitoring to Cloud Factory. This report uses the carve-out method, and the description in section 3 includes only the control objectives and related controls of Cloud Factory and excludes the control objectives and related controls of Netic A/S, Intercom R&D Unlimited Company, Atlassian Pty Ltd, Autho Inc. and Functional Software Inc. Our evaluation did not extend to controls of Netic A/S, Intercom R&D Unlimited Company, Atlassian Pty Ltd, Autho Inc. and Functional Software Inc.

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.

Cloud Factory confirms that:

a) The accompanying description in section 3 fairly presents Cloud Factory's license management platform that has processed personal data for data controllers subject to the data protection rules throughout the period from 23 May 2025 to 31 May 2026. The criteria used in making this statement were that the accompanying description:

   (i) Presents how Cloud Factory's license management platform was designed and implemented, including:

   - The types of services provided, including the type of personal data processed
   - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete and restrict processing of personal data
   - The procedures used to ensure that data processing has taken place in accordance with contract, instructions or agreement with the data controller
   - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality
   - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation
   - The procedures supporting, in the event of breach of personal data security, that the data controller may report this to the supervisory authority and inform the data subjects

Penneo dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

- The procedures ensuring appropriate technical and organisational security measures in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

- Controls that we, in reference to the scope of the license management platform, 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 license management platform for processing personal data in the period from 23 May 2025 to 31 May 2026

(iii) Does not omit or distort information relevant to the scope of the license management platform 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 license management platform 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 23 May 2025 to 31 May 2026. 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 23 May 2025 to 31 May 2026.

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.

Esbjerg, 22 June 2026
Cloud Factory A/S

Jacob Schaumann Schmidt
CEO

Penneo dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

2. Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 23 May 2025 to 31 May 2026 pursuant to the data processing agreement with data controllers

To: Cloud Factory A/S (Cloud Factory) and data controllers

Scope

We have been engaged to report on Cloud Factory's description in section 3 of its license management platform in accordance with the data processing agreement with data controllers throughout the period from 23 May 2025 to 31 May 2026 (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 Cloud Factory has designed and effectively operated suitable controls related to the control objectives stated in section 4. The report does not include an assessment of Cloud Factory'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").

Netic A/S is a subprocessor that provides housing of the primary and secondary data centres to Cloud Factory, and Intercom R&D Unlimited Company, Atlassian Pty Ltd, Autho Inc. and Functional Software Inc. are subprocessors that provide services in the license management platform, ticket system, multifactor authentication and monitoring to Cloud Factory. This report uses the carve-out method, and the description in section 3 includes only the control objectives and related controls of Cloud Factory and excludes the control objectives and related controls of Netic A/S, Intercom R&D Unlimited Company, Atlassian Pty Ltd, Autho Inc. and Functional Software Inc. Our examination did not extend to controls of Netic A/S, Intercom R&D Unlimited Company, Atlassian Pty Ltd, Autho Inc. and Functional Software Inc..

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 Cloud Factory'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.

Cloud Factory's responsibilities

Cloud Factory 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 Cloud Factory 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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

Auditor's responsibilities

Our responsibility is to express an opinion on the fairness of Cloud Factory'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

Cloud Factory's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the licence management platform 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 Cloud Factory's assertion in section 1:

a) The description fairly presents Cloud Factory's license management platform as designed and implemented throughout the period from 23 May 2025 to 31 May 2026

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 23 May 2025 to 31 May 2026, 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 23 May 2025 to 31 May 2026.

Description of test of controls

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

Additional information

The information included in section 5 is presented by Cloud Factory to provide additional information and is not part of Cloud Factory's description of controls that may be relevant to data controllers' internal control as it relates to financial reporting. Such information has not been subjected to the procedures applied in the examination of the description of Cloud Factory's controls and, accordingly, we express no opinion on it.

Penneo dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

Intended users and purpose

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

We permit the disclosure of this report in full only, including the description of tests of controls and results thereof by Cloud Factory, at its discretion, to data controllers who have used Cloud Factory's licence management platform during some or all of the period from 23 May 2025 to 31 May 2026, 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, 22 June 2026
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

Martin Roursgaard Nielsen
Manager

Penneo dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

3. Description of processing

Cloud Factory A/S is a distributor of cloud services, primarily serving customers such as Managed Service Providers ("MSPs") and Independent Software Vendors ("ISVs"). As a cloud distributor, Cloud Factory A/S exclusively delivers services through our self-service portals, the Partner Portal and the Customer Portal. These portals serve as a centralised licence management platform enabling our customers to efficiently manage, provision and adjust their own use of cloud services, as well as that of their end-customers. The license management platform was initially hosted in Cloud Factory's own Infrastructure as a Service environment located in housing facilities provided and protected by GlobalConnect but were later migrated to Netic A/S infrastructure environment.

3.1. Nature of processing

Cloud Factory A/S processes personal data on behalf of the data controller, primarily in connection with the management of the data controller's account, as well as any personal data entered into Cloud Factory A/S's Platform by the data controller or, where applicable, their end customers. Additionally, Cloud Factory A/S may process personal data in the context of providing support services to the data controller, to the extent such data is shared for that purpose.

3.2. Personal data

Cloud Factory A/S processes the categories of personal data that the data controller has explicitly instructed Cloud Factory A/S to process and has specified in the data processing agreement, including:

- Address, email, IP address, name, password, phone number, username for one or several systems, billing and accounting information (only relevant if such information refers to a natural person).

Cloud Factory A/S processes personal data concerning data subjects as expressly instructed by the data controller and as outlined in the data processing agreement, including:

- The data controller's employees
- Employees of the data controller's end customers.

3.3. Practical measures

Secure and responsible data processing is central to the services we provide. We are deeply committed to data protection and particularly compliance with the General Data Protection Regulation (GDPR). To uphold this commitment, we continuously work to strengthen our technical and organisational security measures, ensuring that customer data is handled with the highest level of security.

As part of our security framework, Cloud Factory A/S implements, either directly or through trusted suppliers, the following (non-exhaustive) measures:

- A clearly defined IT security policy
- Guidelines to ensure employee security and awareness
- Asset management protocols, including controls for issuing and returning equipment at the start and end of employment
- Use of encryption to protect data
- Oversight of third-party vendors and documented supervision of sub-processors
- Incident response plans and procedures for handling data breaches

Penneo dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

- Formal data processing agreements with sub-processors
- Regular reviews and updates of risk assessments, policies and procedures
- Continuous awareness training for employees
- Access management based on specific work-related responsibilities.

3.4. Risk assessment

Cloud Factory A/S has carried out a structured assessment of potential risks to the rights and freedoms of data subjects, taking into account the safeguards implemented to mitigate such risks. This risk assessment reflects our commitment to responsible data processing and compliance with the GDPR.

The assessment process includes:

- A thorough identification of risks associated with data processing activities, followed by classification based on their likelihood and potential impact
- An evaluation of whether the technical and organisational measures in place are adequate to ensure compliance with GDPR requirements – and whether this compliance can be clearly documented.

Based on the results of our internal evaluations, Cloud Factory A/S has not identified any high-risk scenarios affecting data subjects across the various data subject types and personal data categories processed.

3.5. Control measures

Cloud Factory A/S has established an annual compliance cycle to systematically monitor and assess the security of personal data processing. The outcomes of the controls conducted as part of this cycle are continuously reviewed and evaluated, at a minimum on a quarterly basis.

Any required or agreed-upon improvements identified through these evaluations are implemented on an ongoing basis. Relevant updates are communicated to data controllers via Statuspage or email. To ensure compliance with the GDPR and the terms of applicable data processing agreements, Cloud Factory A/S has implemented a set of safeguards and controls aligned with the following control objectives:

- **Control objective A**
  Ensure adherence to procedures and controls that guarantee processing of personal data is conducted in accordance with instructions defined in the data processing agreement.
- **Control objective B**
  Ensure the implementation of technical measures that provide appropriate data processing security.
- **Control objective C**
  Ensure the implementation of organisational measures to maintain relevant data processing security.
- **Control objective D**
  Ensure that personal data can be deleted or returned to the data controller when such terms are agreed upon.
- **Control objective E**
  Ensure that personal data is retained only in accordance with the terms agreed upon with the data controller.
- **Control objective F**
  Ensure the use of approved sub-processors only and that appropriate follow-up is conducted to confirm the effectiveness of their technical and organisational measures for protecting data subjects and processing personal data securely.

Penneo dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

- **Control objective G**
  Ensure that personal data is only transferred to third countries or international organisations in accordance with the agreement with the data controller and based on a valid legal basis for the transfer.

- **Control objective H**
  Ensure Cloud Factory A/S is able to assist the data controller with requests from data subjects regarding access, rectification, erasure or restriction of personal data.

- **Control objective I**
  Ensure that any personal data breaches are managed in accordance with the terms of the applicable data processing agreement.

There have been no significant changes to procedures and controls during the period from May 23, 2025 to May 31, 2026.

3.6. Use of sub-processors

Cloud Factory A/S has established procedures and controls to ensure that only approved sub-processors are engaged. In addition, we actively follow up on the technical and organisational measures implemented by sub-processors to safeguard data subjects' rights and to maintain robust data processing security.

When a sub-processor is engaged to perform specific processing activities, Cloud Factory A/S ensures, through a contract or other legal instrument under EU law or applicable national legislation, that the sub-processor is bound by the same data protection obligations as those outlined in the data processing agreement between Cloud Factory A/S and the data controller. This ensures the sub-processor provides sufficient guarantees to implement appropriate technical and organisational measures in a manner that ensures compliance with both the agreement and the GDPR.

Cloud Factory A/S remains responsible for ensuring that any sub-processor complies, at a minimum, with the same data protection standards and requirements to which Cloud Factory A/S is subject.

Cloud Factory A/S uses the sub-processors listed below to support the delivery of its platform:

NAME	ADDRESS	DESCRIPTION OF PROCESSING
Primary sub-processors		
Netic A/S	CVR: 26762642 Alfred Nobels Vej 259220 Aalborg Øst, Denmark.	The sub-processor provides hosting of the license management platform. Data is stored in a secure data centre facility in Denmark.
Intercom R&D Unlimited Company	124-127 St Stephen's Green Dublin D02 C628 CO Dublin	The sub-processor provides a customer service platform, which is integrated into our licence management platform. Data is stored in a secure data centre facility in Ireland.
Atlassian Pty Ltd	341 George Street, Sydney, Australia	The sub-processor manages support inquiries through a ticketing system. Data is stored in a secure data centre facility in Germany.
Auth0 Inc.	100 1st St Suite 150, San Francisco, USA	The sub-processor provides multi-factor authentication for user login to verify identity and ensure access control to the platform. Data is stored in a secure data centre facility in Germany.
Functional Software Inc. ("Sentry")	45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	The sub-processor provides a monitoring service that enables proactive identification and resolution of frontend bugs encountered by partners. Data is stored in a secure data centre facility in Germany.

Penneo dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

3.7. Transfer of personal data to third countries

Any transfer of personal data to third countries or international organisations by Cloud Factory A/S may only be carried out based on a documented instruction from the data controller and must always comply with Chapter V of the GDPR.

Without such documented instruction, Cloud Factory A/S is not permitted, under the terms of the data processing agreement, to:

a) transfer personal data to a data controller or data processor located in a third country or to an international organisation

b) engage a sub-processor located in a third country to process personal data

c) process personal data within a third country.

The data controller's instruction regarding the transfer of personal data to a third country, including the applicable legal basis under Chapter V of the GDPR, is specified in Annex C, section C.6 of the data processing agreement.

3.8. Data subject's rights

Cloud Factory A/S, taking into account the nature of the processing, assists the data controller as far as possible in fulfilling their obligations to respond to requests from data subjects exercising their rights, as outlined in Chapter III of the GDPR. This assistance is provided through the implementation of appropriate technical and organisational measures.

Specifically, Cloud Factory A/S supports the data controller in ensuring compliance with the following obligations:

a) The duty to inform data subjects when personal data is collected directly from them

b) The duty to inform when personal data is not collected directly from the data subject

c) The right of access

d) The right of rectification

e) The right to erasure ("the right to be forgotten")

f) The right of restriction of processing

g) The obligation to notify recipients in connection with rectification or erasure of personal data or restriction of processing

h) The right of data portability

i) The right to object to processing

j) The right not to be subject to a decision based solely on automated processing, including profiling.

Penneo dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

3.9. Handling of personal data breaches

Cloud Factory A/S will notify the data controller without undue delay after becoming aware of a personal data breach.

Where possible, notification to the data controller will occur no later than 24 hours after Cloud Factory A/S becomes aware of the breach, enabling the data controller to fulfil their obligation to report the breach to the competent supervisory authority in accordance with Article 33 of the GDPR.

In accordance with the data processing agreement, Cloud Factory A/S will assist the data controller in fulfilling their obligation to notify the supervisory authority. This assistance includes providing the following information, as required under Article 33(3) of the GDPR:

a) The nature of the personal data breach, including, where possible, the categories and approximate number of data subjects affected, and the categories and approximate number of personal data records concerned

b) The likely consequences of the personal data breach

c) The measures taken or proposed by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Further details on the specific information Cloud Factory A/S provides in support of the data controller's breach notification obligations are outlined in Annex C of the data processing agreement.

3.10. Record of processing activities

Cloud Factory A/S maintains a register of all categories of processing activities carried out on behalf of data controllers. Cloud Factory A/S has ensured that the record of processing activities for each individual data controller includes the following information:

- The name and contact details of the data processor, the data controller, any representatives of the data controller and any appointed data protection officer
- The categories of processing activities performed on behalf of each data controller
- Where applicable, information regarding transfers to third countries or international organisations, including documentation of appropriate safeguards
- Where possible, a general description of the technical and organisational security measures in place.

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

3.11. Complementary controls at data controllers

The data controller is responsible for implementing security measures within their own organisation, including the protection of integrity, confidentiality and availability in data and systems. Cloud Factory A/S recommends that the data controller follows a security framework, such as ISAE 3402, ISO 27001, CIS18 or similar standards, to achieve a high level of security.

To enhance the protection of data and systems, the data controller is encouraged to implement the following complementary actions:

- Access to Cloud Factory A/S's platform and the associated data should be limited to authorised personnel only, using strong authentication methods, restricted user roles and the principle of least privilege to reduce unnecessary access.

Penneo dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

- All relevant internal devices should be protected with up-to-date antivirus and anti-malware software, and these tools should be actively monitored to detect and mitigate potential threats.

- Employees should be regularly trained in security best practices, including recognising phishing attempts, managing strong passwords and handling personal data with care, to minimise the risk of breaches caused by human error.

- The data controller should take steps to ensure that the personal data being processed is kept accurate and current, correcting or removing outdated or incorrect entries as needed.

- The data controller should verify that the instructions issued to Cloud Factory A/S are lawful under applicable data protection regulations.

- The data controller should assess whether the instructions are appropriate and consistent with both the data processing agreement and the main service being provided.

- In cases where support is requested, the data controller should ensure that only the personal data necessary for resolving the support request is shared or made accessible.

- Cloud Factory A/S's general deletion policy is that user data will be deleted after two years of inactivity on the platform. If a user needs to be deleted earlier, it is the data controller's responsibility to notify Cloud Factory A/S about such need for deletion.

Penneo dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory'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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory'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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory'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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory'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.	We have observed that not all network equipment is patched with the most recent software updates. No further 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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory's control activity	Tests performed by PwC	Result of PwC's tests
B.7	System monitoring with an alarm feature has been established for the systems and databases used in the processing of personal data. This monitoring comprises: • Monitoring of uptime and availability • Detection of errors and system failures • Logging and analysis of system activity • Alarms in the event of service interruptions, critical errors, or suspicious activity.	Checked by way of inspection that system monitoring with an alarm feature has been established for systems and databases used in the processing of personal data. Checked by way of inspection that, in a sample of alarms, these were followed up on and that the data controllers were informed thereof as appropriate.	No exceptions noted.
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	Checked by way of inspection that formalised procedures are in place to ensure that transmissions of sensitive and confidential 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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory'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 days of logging that the content of log files is as expected compared to the set-up and that documentation confirms the follow-up performed and the response to any security incidents.
		Checked by way of inspection of a sample of days of logging that documentation confirms the follow-up performed on activities carried out by system administrators and others holding special rights.
			No exceptions noted.

Penneo dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory's control activity	Tests performed by PwC	Result of PwC's tests
B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.	Checked by way of inspection that formalised procedures are in place for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised form. Checked by way of inspection of a sample of development or test databases that personal data included therein are pseudonymised or anonymised. Checked by way of inspection of a sample of development or test databases in which personal data are not pseudonymised or anonymised that this has taken place according to agreement with, and on behalf of, the data controller.	No exceptions noted.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	Checked by way of inspection that formalised procedures are in place for regularly testing technical measures, including for performing vulnerability scans and penetration tests. Checked by way of inspection of samples that 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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory'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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory'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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory'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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory'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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory'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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory's control activity	Tests performed by PwC	Result of PwC's tests
D.1	Written procedures are in place which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller. Checked by way of inspection that procedures are up to date.	No exceptions noted.
D.2	The following specific requirements have been agreed with respect to the data processor's storage periods and deletion routines: • The processor shall delete all personal data processed on behalf of the controller no later than two (2) years after the termination of the main agreement, unless otherwise instructed in writing by the controller. • Notwithstanding the above, the processor shall be obligated to delete the personal data immediately upon the controller's written request, provided such request is made in connection with or following the termination of the main agreement.	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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory'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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory'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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory'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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory'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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory'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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory'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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory'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 dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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

Penneo dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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.	Cloud Factory'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, when a personal data breach occurred, measures were taken to respond to such breach.	No exceptions noted.

Penneo dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

5. Additional information from Cloud Factory A/S

The information included in this section is prepared by Cloud Factory to provide data controllers with further information. The section should not be regarded as a part of the description of processing. The information in this section is not covered by audit procedures performed to assess whether the description of processing is fairly presented, whether the controls supporting the control objectives presented in section 4 have been appropriately designed and whether the controls operated effectively throughout the period. Thus, PwC's opinion in section 2 does not cover the information in section 5.

Response to B.5

The network components referenced under B.5 have intentionally not been updated, as these are fully isolated within the environment and have no connection to the internet. This is specifically documented in our internal procedures, primarily due to the potential downtime that updates may cause to operations. This deviation is no longer relevant after the migration to Netic A/S' hosting environment in October 2025.

Penneo dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

PENNEO

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

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

Jacob Vestergaard Schaumann Schmidt
Kunde
Serienummer: 860e9b43-f2fe-412a-9e6a-fb8be3c54903
IP: 80.62.xxx.xxx
2026-06-22 13:28:15 UTC

Mit ID

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
På vegne af: PricewaterhouseCoopers Statsautoriseret…
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2026-06-22 13:53:24 UTC

Mit ID

Martin Roursgaard Nielsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
PwC-medunderskriver
Serienummer: 906a68c3-bc65-462f-ac13-9174a96af3c1
IP: 83.136.xxx.xxx
2026-06-22 14:17:07 UTC

Mit ID

Penneo dokumentnøgle: HNA7D-LUCHV-9ZE8V-V0W4D-UJ8B8-WKRSD

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

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

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

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