Rackhosting ApS

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 May 2025 to 30 April 2026 pursuant to the data processing agreement with customers

October 2026

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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 14
5. Additional information from Rackhosting ApS 31

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

1. Management's assertion

Rackhosting ApS (Rackhosting) processes personal data on behalf of customers either as a data processor for customers who are data controllers or as a sub-processor where customers are data processors. This statement is limited to general standards for administration as described in the Rackhosting standard contract. Specific matters related to individual customer contracts are not covered.

The accompanying description has been prepared for customers who have used general services 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.

Global Connect A/S and Cibicom A/S are service organisations that provides data centre and network to Rackhosting. This report uses the carve-out method, and the description in section 3 includes only the control objectives and related controls of Rackhosting and excludes the control objectives and related controls of Global Connect A/S and Cibicom A/S. Our evaluation did not extend to controls of Global Connect A/S and Cibicom A/S.

The description indicates that certain control objectives specified in the description can be achieved only if the complementary controls at customers 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 customers.

Rackhosting confirms that:

a) The accompanying description in section 3 fairly presents general services that have processed personal data for customers subject to the data protection rules throughout the period from 1 May 2025 to 30 April 2026. The criteria used in making this statement were that the accompanying description:

   (i) Presents how general services were designed and implemented, including:

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

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

- Controls that we, in reference to the scope of the general services, have assumed would be implemented by customers 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 general services for processing personal data in the period from 1 May 2025 to 30 April 2026

(iii) Does not omit or distort information relevant to the scope of the general services being described for the processing of personal data, while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the general services 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 May 2025 to 30 April 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 1 May 2025 to 30 April 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.

Taastrup, 14 October 2026
Rackhosting ApS

Martin Helms
CEO

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

2. Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 May 2025 to 30 April 2026 pursuant to the data processing agreement with customers

To: Rackhosting ApS (Rackhosting) and customers

Scope

We have been engaged to report on Rackhosting's description in section 3 of its general services in accordance with the data processing agreement with customers throughout the period from 1 May 2025 to 30 April 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 Rackhosting has designed and effectively operated suitable controls related to the control objectives stated in section 4. The report does not include an assessment of Rackhosting'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").

Global Connect A/S and Cibicom A/S are service organisations that provides data centre and network to Rackhosting. This report uses the carve-out method, and the description in section 3 includes only the controls objectives and related controls of Rackhosting and excludes the control objectives and related controls of Global Connect A/S and Cibicom A/S. Our examination did not extend to controls of Global Connect A/S and Cibicom A/S.

The description indicates that certain control objectives specified in the description can be achieved only if the complementary controls at customers contemplated in the design of Rackhosting'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 customers.

We express reasonable assurance in our conclusion.

Rackhosting's responsibilities

Rackhosting 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 Rackhosting 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.

Auditor's responsibilities

Our responsibility is to express an opinion on the fairness of Rackhosting'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.

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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

Rackhosting's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of General services 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 Rackhosting's assertion in section 1:

a) The description fairly presents general services as designed and implemented throughout the period from 1 May 2025 to 30 April 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 1 May 2025 to 30 April 2026, and if customers applied the complementary controls referred to in section 3

c) The controls tested, which together with the complementary controls at customers 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 May 2025 to 30 April 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 describing Rackhosting to provide additional information and is not part of Rackhosting's description of controls that may be relevant to customers's internal control as it relates to data processen. Such information has not been subjected to the procedures applied in the examination of the description of Rackhosting's controls and, accordingly, we express no opinion on it.

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

Intended users and purpose

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

We permit the disclosure of this report in full only, including the description of tests of controls and results thereof by Rackhosting, at its discretion, to customers who have used Rackhosting's General services during some or all of the period from 1 May 2025 to 30 April 2026, who have a sufficient understanding to consider it, along with other information about controls operated by customers themselves, without assuming or accepting any responsibility or liability to customers on our part.

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

Hellerup, 14 October 2026
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Michael Clement
State-Authorised Public Accountant
mne23410

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

3. Description of processing

Introduction

This system description concerns information security and measures relating to Rackhosting's hosting services.

Rackhosting ApS uses GlobalConnect A/S and Cibicom A/S as subcontractors providing the physical data centre facilities in which Rackhosting's systems are located. Neither provider is considered a subprocessor, as they provide colocation services only and do not have access to systems containing data.

Rackhosting ApS manages the infrastructure, hosting platform and monitoring associated with IT operations and hosting activities. In this capacity, it is responsible for ensuring that control systems are implemented and function effectively to prevent and detect errors, including deliberate errors, with a view to complying with contracts and good practice.

This description is limited to the general standards for administration set out in Rackhosting ApS's standard contract. Specific matters relating to individual customer contracts are not covered.

Significant changes in the period

There have not been any significant changes in the period.

Description of Services Covered by the Assurance Report

The services provided by Rackhosting ApS are tailored to several different types of customer. The terms applicable to each customer are set out in contracts based on standard contracts for each business area, which may include individual amendments and options. For certain customers, these terms are specified in operations manuals provided to the customer, which serve as system documentation.

The following areas comprise the services offered by Rackhosting ApS:

Hosting platform:

- OpenStack/KVM virtualisation platform
- Virtuozzo VHI management layer
- Tier 1 Storage Area Network (SAN) – primary and secondary sites
- Tier 2 Storage Area Network (SAN) – primary and secondary sites
- Tier 3 objektstorage/S3 – primary and secondary sites
- Fortinet FortiGate next-generation firewall – primary and secondary sites

Customer-facing services:

- SpamExperts email anti-spam and anti-malware service
- DNS operations (dns1.rackhosting.com, dns2.rackhosting.com and dns3.rackhosting.com)
- Veeam backup services

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

Internal services:

- Zabbix monitoring
- Salt automation
- Service desk ticket management
- ComplyCloud GRC
- Outline – internal documentation
- Active Directory
- Microsoft 365

Based on the scope defined above and the more detailed system description below, Rackhosting ApS considers that it has maintained effective controls in all material respects. Rackhosting ApS recognises that this area is continually evolving and works continuously to develop and improve its procedures and controls.

GDPR work is divided into two areas: the internal area, which concerns all internal processes involving personal data, such as HR, IT, marketing and finance; and the customer-facing area covered by this assurance report, which concerns all areas in which we interact with customers and may potentially come into contact with personal data.

Rackhosting ApS operates IT systems in compliance with applicable legal requirements, including the EU General Data Protection Regulation (GDPR). As a general rule, we do not access customers' personal data.

Management of Compliance with Requirements

Compliance with requirements relating to data protection and the protection of personal data follows the organisational structure already established for IT and information security management.

The organisational and management structure is based on functional departments, with each department head responsible for staff management. Security responsibilities within individual processes are allocated to process owners and those performing the activities. Process owners are responsible for the operation and documentation of the individual processes carried out by employees.

Policies and Organisation

An IT security committee (the RH Security Committee) has been established to ensure alignment between data protection and information security work and the organisation.

The IT Security Committee includes representatives from senior management, middle management and operational staff. The committee reports directly to executive management.

Rackhosting ApS's IT Security Committee comprises:

- CEO/CTO, Partner and Founder, Martin Helms
- Head of Sales and Partner, Philip Hegaard
- Documentation and Compliance, Andreas Overgaard

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

The committee sets standards and establishes the principles and guidelines required to achieve the objectives of the adopted IT security policy.

Members of the IT Security Committee regularly undertake relevant further training in IT security and related matters. IT security is implemented through internal strategy, policies, standards, procedures and guidelines.

The CTO is responsible for the day-to-day management, enforcement and implementation of principles and guidelines, incident handling, and operational activities in accordance with the established guidelines. The CTO is also responsible for communicating the guidelines supporting the IT security policy to each employee.

The committee addresses all IT security and data protection matters of principle. Rackhosting ApS has not appointed a Data Protection Officer (DPO). The IT Security Committee performs DPO-related tasks.

Updates to policies and procedures are communicated to employees. Policies and procedures are available in the ISMS/GRC tool, ComplyCloud, where employees can consult them at any time. If employees identify errors or deficiencies, they report them to the IT security coordinator, who ensures that the necessary corrections are made.

Procedures and Controls

Rackhosting ApS has established a range of policies and procedures that all employees have received and been trained to follow. These include:

• Information security policy

• Personal data policy

• Specific procedures

For each service area and cross-functional process described in the preceding sections, a risk assessment has been performed of the configuration and application in relation to compliance with data subjects' rights, including an assessment of whether appropriate technical and organisational controls have been established in the relevant areas.

Rackhosting ApS has established relevant procedures based on the risk assessment.

Rackhosting ApS does not permit customers to store personal data on Rackhosting's systems unless a data processing agreement has been concluded with the customer, acting as either a controller or a processor. When an agreement is concluded, it is reviewed against a fixed set of checkpoints. All data processing agreements are recorded together with a description of any special requirements imposed by the controller, such as response deadlines or requirements for specific controls. Any special requirements are communicated to the relevant internal teams for implementation when servicing customers.

Technical and Organisational Measures

For technical and organisational measures, reference is made to the ISAE 3402 assurance report.

These measures cover areas such as:

• Human resource security

• Management of information-related assets

• Access control

• Cryptography

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

• Physical and environmental security

• Operations security

• Communications security

• System acquisition, development and maintenance

• Supplier relationships

• Information security incident management

• Emergency response, business continuity and recovery management

Requests from Data controllers

Rackhosting ApS has a procedure for handling and documenting requests from controllers for assistance in addressing data subjects' rights, including access, erasure and rectification.

Requests from controllers relating to rights such as access, erasure and rectification are documented in our support system.

Taking into account the nature of the processing, Rackhosting assists the controller, insofar as this is possible, by implementing appropriate technical and organisational measures to enable the controller to fulfil its obligation to respond to requests to exercise data subjects' rights under the GDPR.

To the extent that Rackhosting ApS processes personal data on behalf of and on the instructions of the controller, Rackhosting assists the controller in ensuring compliance with:

- The obligation to implement appropriate technical and organisational security measures to ensure a level of security appropriate to the risks associated with the processing

- The obligation to notify the supervisory authority (the Danish Data Protection Agency) of a personal data breach without undue delay and, where feasible, no later than 72 hours after the controller has become aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons

- The obligation to inform the affected data subject or subjects of a personal data breach without undue delay where the breach is likely to result in a high risk to the rights and freedoms of natural persons

- The obligation to carry out a data protection impact assessment where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons

- The obligation to consult the supervisory authority (the Danish Data Protection Agency) before processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

Control Activities in the Standard Template Issued by FSR – Danish Auditors and the Danish Data Protection Agency That Are Excluded from Section 4 of the Assurance Report

The following control activities in the standard template issued by FSR – Danish Auditors and the Danish Data Protection Agency are excluded from Section 4 of the assurance report because the processing activities to which they relate are not performed as part of Rackhosting's hosting services or not relevant:

- B.10 – Use of personal data for development and testing: Rackhosting does not use customer personal data for its own development, testing or similar purposes. Any development or testing performed by customers within their hosted environments remains the responsibility of the customer.

- D.1-D.3 - Rackhosting provides hosting infrastructure and data storage capacity. Customers are responsible for managing the data within their applications, including determining when data must be deleted and performing the necessary application-level deletion during the service period and before termination.

  Rackhosting does not have the application-level knowledge of customers' data structures necessary to identify and selectively delete or export individual records. These activities are therefore performed by the customer, unless otherwise expressly agreed.

  Where infrastructure-level deletion is required, Rackhosting will delete the hosted environment in accordance with the relevant Data Processing Agreement and the customer's documented instructions, including in connection with termination.

  This allocation of operational responsibilities does not limit Rackhosting's obligations under applicable data protection legislation or the relevant Data Processing Agreement.

- F.1-F6 - 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. Rackhosting do not have any subprocessors – only service organisations.

- G.1–G.3 – Transfers to third countries or international organisations: Rackhosting does not transfer customer personal data to third countries or international organisations in connection with its hosting services. This also applies to access to such data by external suppliers providing support or remote administration.

These exclusions relate solely to the scope of this assurance report and do not limit Rackhosting's obligations under applicable data protection legislation or its data processing agreements.

Complementary Controls to Be Implemented by Datacontrollers

As part of the delivery of the services, certain controls are assumed to be implemented by data controllers and are essential to achieving the control objectives stated in the description. These include:

- Assessing the implications for personal data protection when modifying existing solutions (privacy by design and privacy by default), and submitting a change request to Rackhosting ApS where relevant

- Assessing and testing new versions of solutions during implementation (change management)

- Configuring and managing their own users in the solution's production environment (identity and access management)

- Configuring and managing access for Rackhosting personnel to the customer's environment (identity and access management)

Penneo dokumentnøgle: Q7C6N-1O9H3-3OOD2-ADLVF-EINGK-QYZC7

- Ensuring that sensitive personal data are not included in support requests submitted to Rackhosting through tickets or other channels

- To delete data when necessary

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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.	Rackhosting'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.	We have noted that no data processing agreements have been signed in the period. No exceptions noted.

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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.	Rackhosting'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: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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.	Rackhosting'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.	We have noted that no data processing agreements have been signed in the period. 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: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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.	Rackhosting'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 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: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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.	Rackhosting's control activity	Tests performed by PwC	Result of PwC's tests
B.7	System monitoring with an alarm feature has been established for the systems and databases used in the processing of personal data.	Checked by way of inspection that system monitoring with an alarm feature has been established for systems and databases used in the processing of personal data. Checked by way of inspection that, in a sample of alarms, these were followed up on and that the data controllers were informed thereof as appropriate.	No exceptions noted.
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	Checked by way of inspection that formalised procedures are in place to ensure that transmissions of sensitive and confidential 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: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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.	Rackhosting's control activity	Tests performed by PwC	Result of PwC's tests
B.9	Rackhosting logs in accordance with the customer's requirements. This includes, at a minimum, logging information about date, users, and information about actions taken by system administrators and others with privileged rights. Log information is protected against manipulation and technical errors and is reviewed on an ongoing basis.	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 dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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.	Rackhosting's control activity	Tests performed by PwC	Result of PwC's tests
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.
B.12	Changes to systems, databases or networks are made consistently with established procedures that ensure maintenance using relevant updates and patches, including security patches.	Checked by way of inspection that formalised procedures are in place for handling changes to systems, databases or networks, including handling of relevant updates, patches and security patches. Checked by way of inspection of extracts from technical security parameters and set-ups that systems, databases or networks have been updated using agreed changes and relevant updates, patches and security patches.	We have found that the build version on the sampled SQL database has not been updated with a new version since November 16, 2022. No further exceptions noted.

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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.	Rackhosting's control activity	Tests performed by PwC	Result of PwC's tests
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.	We have found for 2 out of 2 samples of user terminations that the users' access rights were not removed or disabled in a timely manner. For one user, we have been informed that this is because he has helped after his last working day. For both samples, we have inspected that they have not been logged in after resigning. No further exceptions noted.
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.

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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.	Rackhosting's control activity	Tests performed by PwC	Result of PwC's tests
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 audit reports from service organisations.	No exceptions noted.

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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.	Rackhosting'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: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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.	Rackhosting'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: • Certificates of criminal record	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: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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.	Rackhosting'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.	We have found for 2 out of 2 samples of user terminations that the users' access rights were not removed or disabled in a timely manner. For one user, we have been informed that this is because he has helped after his last working day. For both samples, we have inspected that they have not been logged in after resigning. No further 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.	We have found that one of two employees who resigned did not have a signed confidentiality agreement after termination of employment. The employee was verbally reminded of the terms of the employment agreement, but it does not contain elements regarding continued confidentiality after termination of employment. No further 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.	We have found that during some of the period, weekly awareness trainings have been held. We have been able to see the list of invited employees but have not received documentation of who has participated and what the content has been. No further exceptions noted.

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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.	Rackhosting'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: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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.	Rackhosting'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.	We have noted that there have been no requests in the period. No exceptions noted.

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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.	Rackhosting'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.	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.	We have found that during some of the period, weekly awareness trainings have been held. We have been able to see the list of invited employees but have not received documentation of who has participated and what the content has been. No further exceptions noted.

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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.	Rackhosting'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 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 after the data processor became aware of the personal data breach.	We have noted that there have been no breaches in the period. No exceptions noted.

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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.	Rackhosting's control activity	Tests performed by PwC	Result of PwC's tests
I.4	In the event of a breach of personal data security, Rackhosting will submit documentation to the customer that includes, at a minimum, the actual circumstances of the breach, its effect and scope, and the remedial measures taken.	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 dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

5. Additional information from Rackhosting ApS

The information included in this section is prepared by Rackhosting to provide customers 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.

No.	Rackhosting's control activity	Result of PwC's tests	Management comments
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.	We have found that the build version on the sampled SQL database has not been updated with a new version since November 16, 2022. No further exceptions noted.	Management acknowledges the observation. The observation relates to the build version of the sampled SQL database. Management notes that the observation concerns patch and version management rather than the password and lock-out requirements described in the control activity. Management will review the SQL database version, including vendor support status, relevant security updates and operational dependencies. Based on this review, the database will either be updated through the change management process or handled as a documented risk-based exception with relevant compensating controls. Going forward, SQL database build levels will be included in the regular patch and vulnerability management process to ensure periodic review, documented assessment and follow-up on required updates.

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

No.	Rackhosting's control activity	Result of PwC's tests	Management comments
B. 13 / C.5	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.	We have found for 2 out of 2 samples of user terminations that the users' access rights were not removed or disabled in a timely manner. For one user, we have been informed that this is because he has helped after his last working day. For both samples, we have inspected that they have not been logged in after resigning. No further exceptions noted.	Management acknowledges the observation. We agree that access rights should be removed or adjusted in a timely manner upon termination of employment. In the two samples identified, the accounts were not disabled within the expected timeframe. We note that PwC inspected that the users did not log in after their resignation dates. For one of the users, continued access related to post-employment assistance. Going forward, any such access will be handled as a documented, approved and time-limited exception with defined scope and subsequent removal. Management has strengthened the offboarding process to ensure that all employee terminations trigger a documented access review and removal process across relevant systems. The process includes a checklist, responsible owner, deadline for completion, evidence of access removal and separate approval of any exceptions.

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

No.	Rackhosting's control activity	Result of PwC's tests	Management comments
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.	We have found that one of two employees who resigned did not have a signed confidentiality agreement after termination of employment. The employee was verbally reminded of the terms of the employment agreement, but it does not contain elements regarding continued confidentiality after termination of employment. No further exceptions noted.	Management acknowledges that the established termination procedure was not followed in the case identified. Management has reiterated that the procedure must be followed strictly. Any deviation from the procedure must be documented, including the reasons for the deviation. Management has assessed that a separate written reminder approximately ten months after termination is not necessary in this case. In making this assessment, Management has taken into account the continuing protection of qualifying trade secrets under the Danish Trade Secrets Act. This protection does not depend on a new written reminder upon termination. Management acknowledges that this does not replace the requirement to follow and document the established termination procedure.
C.7 / I.2	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.	We have found that during some of the period, weekly awareness trainings have been held. We have been able to see the list of invited employees but have not received documentation of who has participated and what the content has been. No further exceptions noted.	Management acknowledges that the documentation available for the assurance period was insufficient to demonstrate employee participation and the content of the awareness training provided. A structured programme of recurring awareness training will be introduced from 1 November 2026. The programme will include documented training content and employee participation, with follow-up for employees who do not attend or complete the required training.

Penneo dokumentnøgle: Q7C6N-1O9H3-3O0D2-ADLVF-EINGK-QYZC7

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."

Martin Helms
CEO
På vegne af: Rackhosting ApS
Serienummer: 695570c4-3c3a-4885-a3f2-5478783dca70
IP: 80.208.xxx.xxx
2026-10-14 08:18:40 UTC

Mit ID

Michael Clement
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
På vegne af: PricewaterhouseCoopers Statsautoriseret…
Serienummer: 232c5786-309c-4897-93ea-5c2a6741c1d3
IP: 83.136.xxx.xxx
2026-10-14 08:29:29 UTC

Mit ID

Penneo dokumentnøgle: Q7C6N-1O9H3-3OOD2-ADLVF-EINGK-QYZC7

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.