www.pwc.dk

# *Netic A/S*

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 January 2021 to 31 December 2021 pursuant to data processing agreement in relation to Netic A/S' hosting and operating services

*March 2022*

# Contents

# 1. Management's statement

Netic A/S (Netic) processes personal data on behalf of customers in accordance with data processing agreements.

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

Netic uses the following as subprocessors for hosting services:

- Microsoft Ireland Operations Ltd.
- Amazon Web Services EMEA SARL, Luxembourg
- Google Ireland Limited, Ireland.

This report uses the carve-out method and does not comprise controls that the subsprocessors perform for Netic.

Netic confirms that:

a) The accompanying description in section 3 fairly presents Netic's information security and measures related to hosting and operating services that have processed personal data for data controllers subject to the data protection rules throughout the period from 1 January 2021 to 31 December 2021. The criteria used in making this statement were that the accompanying description:

   (i) Presents how Netic's hosting and operating services were designed and implemented, including:

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

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

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

(ii) Includes relevant information about changes in Netic's hosting and operating services in the processing of personal data in the period from 1 January 2021 to 31 December 2021;

(iii) Does not omit or distort information relevant to the scope of Netic's hosting and operating 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 Netic's hosting and operating services that the individual data controllers might consider important in their particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 January 2021 to 31 December 2021. The criteria used in making this statement were that:

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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 January 2021 to 31 December 2021.

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.

Aalborg, 25 March 2022
Netic A/S

Steen Jensen
CEO

# 2. Independent auditor's report

**Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 January 2021 to 31 December 2021 pursuant to data processing agreement in relation to Netic A/S' hosting and operating services**

To: Netic and their customers

**Scope**

We have been engaged to provide assurance about Netic's description in section 3 of Netic's hosting and operating services in accordance with the data processing agreement with customers throughout the period from 1 January 2021 to 31 December 2021 (the description) and about the design and operating effectiveness of controls related to the control objectives stated in the description.

Our report covers whether Netic has designed and effectively operated appropriate controls related to the control objectives stated in section 4. The report does not include an assessment of Netic'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 uses the following as subprocessors for hosting services:

- Microsoft Ireland Operations Ltd.
- Amazon Web Services EMEA SARL, Luxembourg
- Google Ireland Limited, Ireland.

This report uses the carve-out method and does not comprise controls that the subprocessors perform for Netic.

We express reasonable assurance in our conclusion.

**Netic's responsibilities**

Netic is responsible for: preparing the description and accompanying statement in section 1, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives and designing and effectively operating controls to achieve the stated control objectives.

**Auditor's independence and quality control**

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

PricewaterhouseCoopers is subject to the International Standard on Quality Control (ISQC 1) and accordingly uses and maintains a comprehensive system of quality control, including documented policies and 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 Netic's description and on the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures.

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

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

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

**Limitations of controls at a data processor**

Netic's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of their hosting and operating services that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect all personal data breaches. Furthermore, the projection of any evaluation of the operating effectiveness to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

**Opinion**

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the Management's statement section. In our opinion, in all material respects:

a) The description fairly presents Netic's information security and measures related to hosting and operating services as designed and implemented throughout the period from 1 January 2021 to 31 December 2021;

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 January 2021 to 31 December 2021; and

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 January 2021 to 31 December 2021.

**Description of test of controls**

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

**Intended users and purpose**

This report and the description of tests of controls in section 4 are intended only for data controllers who have used Netic's hosting and operating services and who have a sufficient understanding to consider it, along with other information, including information about controls operated by the data controllers themselves, in assessing whether the requirements of the data protection rules have been complied with.

Aarhus, 25 March 2022
**PricewaterhouseCoopers**
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

Rico Lundager
Senior Manager

# 3. Description of Netic's hosting and operating services

## 3.1 Introduction

Netic's primary business areas are hosting, operation/outsourcing, security, consultancy services and technical software development. Netic's customers range from small companies to large organisations; Netic serves as a direct contact for customers, as a partner or as a sub-supplier.

Netic employs approximately 138 people, and Trifork A/S is the majority shareholder of Netic A/S.

## 3.2 Description of services covered by the report

Netic provides operation and hosting to customers within a wide range of fields and products, including related consultancy services.

As Netic has core competencies in a wide range of subject areas, offers many different products and has a high degree of agility. The company is able to resolve large-scale issues at very short notice.

Netic also provides hosting of servers at many different levels, ranging from a single server hosted in our data centre, to which we merely provide power, cooling and internet access; larger farms of virtual/physical servers, operating high-end solutions in full two-centre operation with redundant databases as backends; to operation in public clouds.

Netic also provides customised solutions, designed to meet the needs of each individual customer, on the basis of core competencies and agility. Netic also has a small portfolio of proprietary solutions.

As standard products/services, Netic offers e.g. virtual servers, Kubernetes solutions, infrastructure, hosting of mail, web, applications and databases on self-operated platforms.

Netic uses sub-suppliers if our customers request it. Only recognised and well-reputed providers are used. The following hosting sub-suppliers are used:

- Microsoft Ireland Operations Ltd.
- Amazon Web Services EMEA SARL, Luxembourg
- Google Ireland Limited, Ireland.

*When entering into agreements for which sub-suppliers in third countries are used, Netic has prepared a disclaimer pointing out to the customer that entering into such an agreement is contrary to the Schrems 2 judgement – and the customer is informed of any consequences thereof.*

## 3.3 General control environment

Netic has set up a security committee that focuses on continuously ensuring the protection of personal data. The committee consists of the CEO, COO, the CTO, the operations manager and the DPO/CISO. The committee meets regularly and reviews the current data protection level; this includes a discussion of IT security initiatives to increase the IT security level at Netic. The committee has been put together to unite relevant experts in ensuring the GDPR work, and responsibilities are allocated based on the members' competences.

The work of the committee is planned in a GDPR year plan comprising relevant activities to ensure that Netic is always compliant according to applicable law.

When the committee meets, the following topics are discussed:

- IT security policy and IT security manual
- Privacy policies and procedures
- IT security measures
- Review of any security breaches
- Follow-up on training and awareness.
- As regards concluded data processing agreements:
    - Follow-up on receipt of (new) data processing agreements and approval of them
    - Follow-up on customers with special requirements in their data processing agreements
    - Follow-up on approval of potential sub-suppliers
    - Follow-up to verify that the data controller has approved any procedures and technical measures that ensure the processing and protection of personal data
    - Follow-up to verify that enquiries from the data controller with regard to the rights of data subjects (access, erasure, rectification) have been handled in an appropriate and timely manner.
- As regards any incidents occurred:
    - Follow-up to verify that incidents have been reported satisfactorily to the data controller in a timely manner.

Netic has appointed a DPO (data protection officer) whose primary work is to ensure that personal data is processed in accordance with applicable law. The DPO also acts as Netic's CISO.

The data protection officer works in the cross field between legal requirements, the use of personal data and information security.

The data protection officer's overall tasks are as follows:

- Provide advice and recommendations on rights and obligations relating to data processing
- Supervise correct data protection
- Handle requests from data subjects regarding their personal data
- Keep Management informed of its obligations under the Data Protection Act
- Act as primary contact for supervisory authorities
- Be responsible for the process for handling personal data breaches and for notifying relevant authorities of any leaks of personal data
- Become involved in the implementation of new systems, services, workflows etc. in which personal data are processed
- Ensure ongoing and provable compliance.

The data protection officer exercises his or her activities independently, meaning that the data protection officer is not instructed on how to perform his or her tasks. The data protection officer reports directly to Netic's Executive Board. Reporting is provided at least annually following a formal process.

Netic's IT security policy and privacy policy (customer-facing) apply to all Netic employees and are part of the basis of the employment relationship. The policies provide the framework for the processing, storage, sharing and erasure of data, and they contain procedures for rights management, password management, patching, logging, backup, access control, etc.

The policies are updated at specified intervals and, as a minimum, when the company introduces new systems, services, business processes etc. of importance to the security or data protection.

All documents relating to data protection, including documentation, risk analyses, policies, reports, etc., are placed on Netic's intranet. Access to this space is restricted so that only relevant employees have access to information about the handling and follow-up on the data controller's enquiries/requests for support, e.g. support for responding to a request from a data subject (the end user) regarding his or her rights, as well as the data controller's enquiries regarding impact assessment and consultation with the supervisory authority. Likewise, only relevant employees and members of the security committee have access to the documentation/analysis in the event of a security breach.

The operations manager and the data protection officer are responsible for checking that the required controls are carried out and have the intended effect. The results are discussed by Management, and any necessary actions are agreed.

## 3.4 Significant changes

During the period from 1 January 2021 to 31 December 2021, no significant changes have been made to Netic's operations that may affect the security and operational stability of our customers.

## 3.5 Risk assessment

Netic has formalised processes for assessing the risk of the services in which personal data are processed.

The risk assessment is reviewed at specified intervals and, additionally, as a minimum when a system is modified significantly, new business processes are implemented, a new central system is applied or when we process new types of personal data as part of our services.

The focal point of the risk assessments is the risk/likelihood of a personal data breach and the consequences to the data subject of such a breach.

The risk assessments help ensure that we have determined whether the necessary technical and organisational security measures are always set up to protect the data being processed for our customers. The risk assessments are thus used in the continued effort to establish organisational and technical security measures to counter the risks (risk management) stated in the risk assessment.

Risk assessments are made by the security committee with input from relevant employees of the organisation.

### *The current risk landscape*

Considering the data we process – together with the controls and the organisational and technical measures we have implemented to mitigate risks and minimise the likelihood of personal data breaches – the current risk profile of Netic's services is assessed as being low. To ensure a constant focus on minimising our risks, we have established control activities aiming at both safeguarding and testing that our measures adequately mitigate risks.

## 3.6 Control activities

The description of Netic's control environment is divided into the following topics:

### *Information security policies*

Netic endeavours to ensure that relevant controls are based on the ISO 27001 standard, and they are described in Netic's IT security policy.

## Employee security

Netic provides continuous training to all employees within IT security and safe processing of personal data.

Any change to Netic's IT security policies and privacy policies will be communicated to all employees. New employees are required to read policies and manuals prior to reviewing these together with Netic's DPO in order to get answers to their questions and to establish their security awareness at an appropriate level. Netic requires all employees at Netic to have a clean criminal record.

Relevant training and awareness activities are added over the year, e.g. by using Netic's proprietary GDPR test and examination system where the employee is introduced to and trained in relevant topics within personal data and IT security.

Every year, the company makes an internal evaluation as to whether the awareness training and the ongoing training have had the desired effect. The results are evaluated by the security committee.

## Access control

Netic's general policy on access to systems is that access is only allowed if it serves a legitimate purpose. This applies to physical as well as logical access. Where technically feasible, all access to systems must be logged with accurate information on time and identification of the user who accessed the system in question. Those of Netic's employees being part of the 24/7 duty system have access to all operations-critical systems as this is required to maintain a 24/7 contingency preparedness. All other access is granted only when there is an essential and imperative need. Customers only have access to their own systems. For systems that contain sensitive personal data, they often only have access to a limited part of the system so that data security is maintained, and access is limited as much as possible. Some systems require segregation of duties, and other conditions for access may consequently exist. These conditions are documented for the individual systems.

## Managing assets and systems

New assets are registered in Netic's fixed assets register and/or CMDB depending on the nature of the asset. All assets are kept in good security condition through support agreements, upgrade of software and firmware to secure versions, ongoing patch management according to the customer contract and Netic's patch management policy, etc.

Netic has a policy on the destruction of data dictating that when abolishing assets, storage media will be destroyed on location and will not be returned with data to a manufacturer for service, upgrading or the like.

## Cryptography

All data connections transmitting confidential, personal or sensitive data must be strongly encrypted with up-to-date technology.

Data extracts containing sensitive data transmitted between Netic and Netic's customers and/or business partners must be encrypted, only allowing the intended party to open them. For this purpose, Netic recommends the use of PGP. Data extracts include all types of sensitive data on all types of media – for example DVDs, USB sticks, emails and digital uploads.

## Physical and environmental security

Customer data is stored on IT systems in Netic's data centres. These data centres are protected by electronic access control with two-factor access, electronic burglary monitoring by a security firm, video surveillance and several layers of physical security. Internally in the data centres, customers, who themselves have access, are physically separated, and certain critical systems are moreover physically separated from the ordinary operational systems.

## Operations security

The management team responsible for the day-to-day operation of Netic consists of Steen Jensen, CEO, John Zimmer, COO, Claus Hansen, CCO, Henrik Skovfoged, TS Business Unit Lead, and Karsten Thygesen, CTO.

Where technically feasible and financially reasonable, the design of all IT systems, e.g. networks, servers, IT systems and the like, is based on the principle of no single point of failure.

All data centres are physically placed in buildings with a high security level and several layers of physical security. The data centres are protected against operational loss incidents through the use of aspiration systems and Inergen-based fire suppression, battery/UPS backup, generator-based emergency power and redundant power supply for equipment.

Redundant internet connections from several ISPs always exist – all of them in cables carried in different routings – inside as well as outside the buildings. Furthermore, the data centres are connected internally by several fibre cables carried by different routings and with different routings in the buildings.

All critical data centre components are monitored 24/7 by an internal SOC function.

Netic has prepared and maintains contingency plans describing principles for decision-making power, organisation, communication and remediation of unexpected emergency situations. Furthermore, the contingency plans contain descriptions of a number of options in case of different well-reasoned scenarios to be able to get back to normal operations as quickly as possible. The contingency plans cover physical problems such as fire, water, theft, vandalism, power outage etc. as well as logical problems such as data loss, logical breakdowns, hacking and data theft. The contingency plans are maintained on an ongoing basis and are tested through contingency exercises.

## Acquisition, development and maintenance of systems

The development, operation and maintenance of systems are always based on the security requirements for the processing of data to ensure that data is protected during processing, transportation and storage. Systems are maintained through high-frequency automated patch management with the option of extra patching in emergency situations. Routine vulnerability scans are conducted, and employees are continuously informed and updated on security requirements and procedures applicable when working on systems with sensitive data.

## Supplier relationships

All suppliers of Netic must comply with Netic's IT security policy and privacy policy and must be instructed in Netic's IT security manual to the extent necessary. If a supplier needs access – whether physical or logical – to systems containing customer data, the supplier will be closely accompanied by a Netic employee.

## Information security incident management

As described in Netic's IT security policy:

*"If an employee detects threats to information security or breaches of it, this must immediately result in the creation of an Incident in Netic's incident reporting system and be reported to Netic's CISO/DPO."*

## Information security aspects of business continuity management

In emergency or recovery situations, Netic's IT security policy and privacy policies are still applicable and cannot be set aside at any time.

## *Monitoring*

Reporting to the Executive Board is done on an ad hoc basis. The reporting includes status on the GDPR work, follow-up on the receipt and approval of (new) data processing agreements and follow-up to verify that the enquiries from the data controller with regard to the rights of data subjects (access, erasure, rectification) have been handled in an appropriate and timely manner.

# *3.7 Complementary controls of data controllers*

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

- Setting up and administering own users of the solution in the production environment (identity and access management)
- Setting up and administering users from Netic who have access to the customer's environment (identity and access management)
- Ensuring that sensitive personal information is not included in support cases sent to Netic via tickets etc.

# 4. Control objectives, control activity, tests and related findings

## 4.1 Purpose and scope

We have conducted our engagement in accordance with ISAE 3000, "Assurance engagements other than audits or reviews of historical financial information", and additional requirements under Danish audit regulation.

Our testing of the design, implementation and functionality of the controls has included the control objectives and related control activities selected by Management and listed in section 4.3. Any other control objectives, related controls and controls at customers are not covered by our test actions.

Our operating effectiveness testing included the control activities deemed necessary to obtain reasonable assurance that the stated control activities were achieved in the period from 1 January 2021 to 31 December 2021.

## 4.2 Test actions

The test actions performed when determining the operating effectiveness of the control activities are described below:

| | |
|---|---|
| *Inspection* | Reading of documents and reports containing specifications regarding the execution of the control. This includes reading and consideration of reports and other documentation in order to assess whether specific controls are designed so they may be expected to become effective, if implemented. Furthermore, it is assessed whether controls are being monitored and checked sufficiently and at appropriate intervals.<br>We have tested the specific system set-up on the technical platforms, databases and network components in order to verify whether controls are implemented and have functioned in the period from 1 January 2021 to 31 December 2021. Among other things, this includes assessment of patching level, permitted services, segmentation, password complexity, etc. as well as inspection of equipment and locations. |
| *Inquiries* | Inquiry of appropriate personnel. Inquiries have included how the controls are performed. |
| *Observation* | Observation of the execution of the control. |
| *Reperformance of the control* | Repetition of the relevant control. We have repeated the execution of the control to verify that the control functions as assumed. |

## 4.3 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 consistently with the data processing agreement entered into.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| A.1 | Written procedures are in place which include a requirement that personal data must only be processed when instructions to this effect are available.<br>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.<br>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.<br>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.<br>Checked by way of inspection of a sample of personal data processing operations that these are conducted consistently with instructions. | No exceptions noted. |
| 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.<br>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.<br>Checked by way of inspection that the data controller was informed in cases where the processing of personal data was evaluated to be against legislation. | No exceptions noted. |

**Control objective B:**

*Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.1 | Written procedures are in place which include a requirement that security measures agreed are established for the processing of personal data in accordance with the agreement with the data controller.<br>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.<br>Checked by way of inspection that procedures are up to date.<br>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.<br>Checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data.<br>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.<br>Checked by way of inspection that the data processor has implemented the security measures agreed with the data controller. | During our audit, we observed that several projects have not been risk-assessed based on risks to the data subject. Furthermore, it is not clear when a risk assessment has been carried out and whether the necessary technical and organisational security measures have been established.<br>No further 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.<br>Checked by way of inspection that antivirus software is up to date. | No exceptions noted. |

**Control objective B:**

*Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.4 | External access to systems and databases used in the processing of personal data takes place through a secured firewall. | Checked by way of inspection that external access to systems and databases used in the processing of personal data takes place only through a secured firewall.<br>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.<br>Inspected network diagrams and other network documentation to ensure appropriate segmentation. | During our audit, we observed that filters have been set up that only allow access to customer networks for employees with a work-related need. However, a legacy network still exists that allows access to customer networks for all employees. We have been informed that the legacy network was closed on 14 June 2021.<br><br>No further exceptions noted. |

**Control objective B:**

*Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.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.<br>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.<br>Checked by way of inspection that the technical measures agreed support retaining the restriction in users' work-related access to personal data.<br>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. | During our audit, we observed that selected customer servers do not comply with Netic's internal password policy.<br>During our audit of selected customer servers, we observed that the lockout policy does not follow a baseline.<br>During our audit of privileged access, we were informed that privileged access is granted through membership of a group. We were informed that a centralised list of systems to which the groups provide access is not maintained.<br>No further exceptions noted. |
| B.7 | System monitoring has been established for the systems and databases used in the processing of personal data, e.g. in the event of a compromise. | Checked by way of inspection that system monitoring with an alarm feature has been established for systems and databases used in the processing of personal data.<br>Checked by way of inspection of a sample of alarms that these were followed up on and that the data controllers were informed thereof as appropriate. | No exceptions noted. |

**Control objective B:**

*Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.8 | Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email. | Checked by way of inspection that formalised procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognised algorithm.<br>Checked by way of inspection that technological encryption solutions have been available and active throughout the assurance period.<br>Checked by way of inspection that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.<br>Inquired whether any unencrypted transmission of sensitive and confidential personal data has taken place during the assurance period and whether the data controllers have been appropriately informed thereof. | No exceptions noted. |

**Control objective B:**

*Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.9 | Logging of the following matters has been established in systems, databases and networks:<br>• Activities performed by system administrators and others holding special rights<br>• Security incidents comprising:<br>  ○ Changes in log set-ups, including disabling of logging<br>  ○ Changes in users' system rights<br>  ○ Failed attempts to log on to systems, databases or networks.<br>Logon data are protected against manipulation and technical errors and are reviewed regularly. | Checked by way of inspection that formalised procedures are in place for setting up logging of user activities in systems, databases or networks that are used to process and transmit personal data, including review of and follow-up on logs.<br>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.<br>Checked by way of inspection that user activity data collected in logs are protected against manipulation or deletion.<br>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.<br>Checked by way of inspection of a sample of logging that documentation confirms the follow-up performed on activities carried by system administrators and others holding special rights. | No exceptions noted. |
| 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.<br>Checked by way of inspection of a sample of development or test databases that personal data included therein are pseudonymised or anonymised.<br>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. | We have been informed that development activity is not performed at Netic. |

**Control objective B:**

*Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.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.<br>Checked by way of inspection of samples that documentation confirms regular testing of the technical measures established.<br>Checked by way of inspection that any deviations or weaknesses in the technical measures have been responded to in a timely and satisfactory manner and communicated to the data controllers as appropriate. | No exceptions noted. |
| 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.<br>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. |

**Control objective B:**

*Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.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.<br>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.<br>Checked by way of inspection of a sample of resigned or dismissed employees that their access to systems and databases was deactivated or removed in a timely manner.<br>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. | During our audit, we observed that an assessment of privileged accounts has been performed within the period. We have been informed that the design of the control does not include a formal update of access before it is approved.<br>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.<br>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.<br>Checked by way of inspection of documentation that, throughout the assurance period, only authorised persons have had physical access to premises and data centres at which personal data are stored and processed. | No exceptions noted. |

**Control objective C:**

*Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| C.1 | Management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The information security policy is based on the risk assessment performed.<br>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.<br>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.<br>Checked by way of inspection of a sample of data processing agreements that the requirements in these agreements are covered by the requirements of the information security policy for security measures and security of processing. | No exceptions noted. |

**Control objective C:**

*Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| C.3 | The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant:<br>• References from former employers<br>• Certificates of criminal record<br>• 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.<br>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.<br>Checked by way of inspection of employees appointed during the assurance period that documentation states that the screening has comprised:<br>• References from former employers<br>• Certificates of criminal record<br>• 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.<br>Checked by way of inspection of employees appointed during the assurance period that the relevant employees have been introduced to:<br>• The information security policy<br>• Procedures for processing data and other relevant information. | No exceptions noted. |

**Control objective C:**

*Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| C.5 | 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.<br>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.<br>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.<br>Inspected documentation stating that all employees who have either access to or process personal data have completed the awareness training provided. | No exceptions noted. |

**Control objective D:**

*Procedures and controls are complied with to ensure that personal data can be deleted or returned if arrangements are made with the data controller to this effect.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| D.1 | Written procedures are in place which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller.<br>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.<br>Checked by way of inspection that procedures are up to date. | No exceptions noted. |
| D.2 | Any agreed specific requirements for the data processor's storage periods and deletion routines in accordance with the concluded data processing agreements are followed. | Checked by way of inspection that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines.<br>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.<br>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:<br>• Returned to the data controller and/or<br>• 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.<br>Checked by way of inspection of terminated data processing sessions during the assurance period that documentation states that the agreed deletion or return of data has taken place. | No exceptions noted. |

**Control objective E:**

*Procedures and controls are complied with to ensure that the data processor will only store personal data in accordance with the agreement with the data controller.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| E.1 | Written procedures are in place which include a requirement that personal data must only be stored in accordance with the agreement with the data controller.<br>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.<br>Checked by way of inspection that procedures are up to date.<br>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.<br>Checked by way of inspection of a sample of data processing sessions from the data processor's list of processing activities that documentation states that the processing of data, including the storage of personal data, takes place only in the localities stated in the data processing agreement – or otherwise as approved by the data controller. | No exceptions noted. |

**Control objective F:**

*Procedures and controls are complied with to ensure that only approved subprocessors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| F.1 | Written procedures are in place which include requirements for the data processor when using subprocessors, including requirements for subprocessing agreements and instructions.<br>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.<br>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.<br>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.<br>Inspected documentation stating that the data controller was informed when changing the subprocessors used throughout the assurance period. | No exceptions noted. |
| 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.<br>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. |

**Control objective F:**

*Procedures and controls are complied with to ensure that only approved subprocessors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| F.5 | The data processor has a list of approved sub-processors disclosing:<br>• Name<br>• Company registration no.<br>• Address<br>• Description of the processing. | Checked by way of inspection that the data processor has a complete and updated list of subprocessors used and approved.<br>Checked by way of inspection that, as a minimum, the list includes the required details about each subprocessor. | No exceptions noted. |
| 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.<br>Checked by way of inspection of documentation that each subprocessor and the current processing activity at such processor are subjected to risk assessment.<br>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.<br>Checked by way of inspection of documentation that information on the follow-up at subprocessors is communicated to the data controller so that such controller may plan an inspection. | No exceptions noted. |

**Control objective G:**

*Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| G.1 | Written procedures are in place which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.<br>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.<br>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.<br>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.<br>Checked by way of inspection that procedures are up to date.<br>Checked by way of inspection of a sample of data transfers from the data processor's list of transfers that documentation confirms a valid basis of transfer in the data processing agreement with the data controller and that transfers have only taken place insofar as this was arranged with the data controller. | No exceptions noted. |

**Control objective H:**

*Procedures and controls are complied with to ensure that the data processor can assist the data controller in handing out, correcting, deleting or restricting information on the processing of personal data to the data subject.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| H.1 | Written procedures are in place which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects.<br>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.<br>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:<br>• Handing out data<br>• Correcting data<br>• Deleting data<br>• Restricting the processing of personal data<br>• Providing information about the processing of personal data to data subjects.<br>Checked by way of inspection of documentation that the systems and databases used support the performance of the relevant detailed procedures. | No exceptions noted. |

**Control objective I:**

*Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| I.1 | Written procedures are in place which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches.<br>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.<br>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:<br>• Awareness of employees<br>• Monitoring of network traffic<br>• 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.<br>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.<br>Checked by way of inspection of documentation that logging of access to personal data, including follow-up on repeated attempts to gain access, is followed up on in a timely manner. | No exceptions noted. |

**Control objective I:**

*Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.*

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| I.3 | If any personal data breach occurred, the data processor informed the data controller without undue delay and in accordance with the data processing agreement after having become aware of such personal data breach at the data processor or a subprocessor. | Checked by way of inspection that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach.<br>Made inquiries of the subprocessors as to whether they have identified any personal data breaches throughout the assurance period.<br>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.<br>Checked by way of inspection that all personal data breaches recorded at the data processor or the subprocessors have been communicated to the data controllers concerned without undue delay and in accordance with the data processing agreements after the data processor became aware of the personal data breach. | No exceptions noted. |
| 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:<br>• The nature of the personal data breach<br>• Probable consequences of the personal data breach<br>• 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:<br>• Describing the nature of the personal data breach<br>• Describing the probable consequences of the personal data breach<br>• Describing measures taken or proposed to be taken to respond to the personal data breach.<br>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. |

# 5. Additional information from Netic

The information included in this section is prepared by Netic to provide the customer with further information. The section should not be regarded as a part of the system description. The information in this section is not covered by audit procedures performed to assess whether the system description gives a true and fair view, whether the controls supporting the control objectives presented in section 4 have been suitably designed and whether they operated effectively throughout the period. Thus, PwC's conclusion in section 3 does not cover the information in section 5.

Under the control activity B2, PwC states:

"During our audit, we observed that several projects have not been risk-assessed based on risks to the data subject. Furthermore, it is not clear when a risk assessment has been carried out and whether the necessary technical and organisational security measures have been established".

For this observation, Netic states that a formal risk assessment is completed in Netic's shared infrastructure elements in 2021, also with focus on the data subjects. It is correct that some projects have not been risk-assessed separately. In March 2022, all new projects will be assessed according to the ISO 27001 framework.

There have been no records of data breaches in 2021.

Under the control activity B5, PwC states:

"During our audit, we observed that filters have been set up that only allow access to customer networks for employees with a work-related need. However, a legacy network still exists that allows access to customer networks for all employees. We have been informed that the legacy network was closed on 14 June 2021.

For this observation, Netic states that the legacy network was closed on 14 June 2021.

Under the control activity B6, PwC states:

"During our audit, we observed that selected customer servers do not comply with Netic's internal password policy.

During our audit of selected customer servers, we observed that the lockout policy does not follow a baseline.

During our audit of privileged access, we were informed that privileged access is granted through membership of a group. We were informed that a centralised list of systems to which the groups provide access is not maintained".

For this observation, Netic states that during 2021 all root accounts were set with individual passwords with special password requirements that differ a bit from standard requirements for practical reasons. Securing the root account is a major step in improving security as the local user is only used on a limited number of servers. Action for rolling out the required software for enforcing specific local user password rules is still ongoing. The lockout policy is "After five failed logon attempts, the security incident is handled by Netic SOC. The SOC is manned 24/7/365. The process is not fully implemented for all servers.

Under the control activity B13, PwC states:

" During our audit, we observed that an assessment of privileged accounts has been performed within the period. We have been informed that the design of the control does not include a formal update of access before it is approved".

For this observation, Netic will update the design and process in 2022.

PENNEO

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

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

**Steen Jensen**
**Kunde**
På vegne af: Netic A/S
*Serienummer: PID:9208-2002-2-013933737584*
*IP: 77.243.xxx.xxx*
*2022-03-25 10:15:19 UTC*
NEM ID

**Rico Lundager**
**Revisor**
På vegne af: PricewaterhouseCoopers Statsautoriseret…
*Serienummer: CVR:33771231-RID:30016557*
*IP: 208.127.xxx.xxx*
*2022-03-25 10:18:50 UTC*
NEM ID

**Jesper Parsberg Madsen**
**Statsautoriseret revisor**
På vegne af: PricewaterhouseCoopers Statsautoriseret…
*Serienummer: PID:9208-2002-2-427963640472*
*IP: 80.62.xxx.xxx*
*2022-03-25 10:30:54 UTC*
NEM ID