

Novicell ApS

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 June 2022 to 31 May 2023 pursuant to the data processing agreement with data controllers

November 2023



Contents

1. Management’s statement	3
2. Independent auditor’s report.....	5
3. Description of processing.....	8
4. Control objectives, control activities, tests and related findings	12

1. Management's statement

Novicell ApS processes personal data on behalf of data controllers in accordance with the data processing agreement.

The accompanying description has been prepared for data controllers who has used Novicell ApS' services and who has 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.

Novicell ApS uses Dynamicweb Software A/S, Curanet A/S, Platform.sh SAS, Umbraco A/S, WP Engine Inc. and Microsoft as subprocessors for operation and hosting. This report uses the carve-out method and does not comprise control objectives and controls that Dynamicweb Software A/S, Curanet A/S, Platform.sh SAS, Umbraco A/S, WP Engine Inc. and Microsoft Azure perform for Novicell ApS.

Some of the control objectives stated in our description in section 3 can only be achieved if the complementary controls at data controllers are suitably designed and operating effectively with our controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

Novicell ApS confirms that:

- a) The accompanying description in section 3 fairly presents Novicell ApS' services that has processed personal data for data controllers subject to the data protection rules throughout the period from 1 June 2022 to 31 May 2023. The criteria used in making this statement were that the accompanying description:
 - (i) Presents how Novicell ApS' services was designed and implemented, including:
 - The types of services provided, including the type of personal data processed;
 - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete and restrict processing of personal data;
 - The procedures used to ensure that data processing has taken place in accordance with contract, instructions or agreement with the data controller;
 - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality;
 - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation;
 - The procedures supporting, in the event of breach of personal data security, that the data controller may report this to the supervisory authority and inform the data subjects;
 - 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 Novicell ApS' services, have assumed would be implemented by the data controllers and which, if necessary in order to achieve the control objectives stated in the description, are identified in the description;
 - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data.
- (ii) Includes relevant information about changes in the data processor's Novicell ApS' services in the processing of personal data in the period from 1 June 2022 to 31 May 2023;
- (iii) Does not omit or distort information relevant to the scope of Novicell ApS' 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 Novicell ApS' 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 June 2022 to 31 May 2023. 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 June 2022 to 31 May 2023.
- c) Appropriate technical and organisational measures were established and maintained to comply with the agreements with the data controllers, sound data processing practices and relevant requirements for data processors in accordance with the data protection rules.

Aarhus, 3. November 2023
Novicell ApS

Kristian Rasmussen
CFO

2. Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 June 2022 to 31 May 2023 pursuant to data processing agreements with data controllers

To: Novicell ApS and Novicell ApS' customers

Scope

We have been engaged to provide assurance about Novicell ApS' description in section 3 of services in accordance with the data processing agreement with data controllers throughout the period from 1 June 2022 to 31 May 2023 (the description) and about the design and operating effectiveness of controls related to the control objectives stated in the description.

Our report covers whether Novicell ApS has designed and effectively operated suitable controls related to the control objectives stated in section 4. The report does not include an assessment of Novicell ApS' 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").

Novicell ApS uses Dynamicweb Software A/S, Curanet A/S, Platform.sh SAS, Umbraco A/S, WP Engine Inc. and Microsoft as subprocessors for operation and hosting. This report uses the carve-out method and does not comprise control objectives and controls that Dynamicweb Software A/S, Curanet A/S, Platform.sh SAS, Umbraco A/S, WP Engine Inc. and Microsoft Azure perform for Novicell ApS.

Some of the control objectives stated in Novicell ApS' description in section 3 can only be achieved if the complementary controls at data controllers are suitably designed and operating effectively with Novicell ApS' controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

We express reasonable assurance in our conclusion.

Novicell ApS' responsibilities

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

Auditor's independence and quality control

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

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

Auditor's responsibilities

Our responsibility is to express an opinion on Novicell ApS' 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 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

Novicell ApS' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of 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 Novicell ApS' services as designed and implemented throughout the period from 1 June 2022 to 31 May 2023;
- b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 June 2022 to 31 May 2023; 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 June 2022 to 31 May 2023.

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 Novicell ApS' 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, 3. November 2023

PricewaterhouseCoopers

Statsautoriseret Revisionspartnerselskab

Jesper Parsberg Madsen

State-Authorised Public Accountant

mne26801

3. Description of processing

Introduction

This system description relates to the personal data protection controls for consultancy services and hosting activities at Novicell ApS including Novicell Design ApS, named Novicell in this description.

As a consultancy agency and hosting provider, Novicell is responsible for implementing control systems that protect personal data in order to live up to legal responsibilities, contractual obligations and good practice.

This description is limited to the general standards for our services as described in Novicell's standard contract. Specific conditions – related to individual customer contracts – are not included.

Description of services

Novicell's services are tailored to the specific customer, and the specific customer terms are described in individual contracts. For each service area, a standard contract is used as the foundation, and individual adjustments and addendums can be included. Processing activities of personal data are agreed upon in a data protection agreement that includes any customer-specific requirements. Customers can buy services from one or more areas. The following service areas represent the services that Novicell offers:

Hosting: Customers hosted on dedicated hardware, dedicated virtualised servers or shared servers. Novicell is responsible for networking, backup and system software. Physical security responsibility is assigned to a housing partner.

Cloud hosting: Customers hosted with public cloud providers. Novicell is responsible for backup, configuration of services and/or system software. Networking and physical security responsibility are assigned to a cloud provider.

Consultancy: Customers who hire Novicell consultants (development, design, strategy, enterprise architecture) to work under customer direction. Novicell is responsible for the consultant's general personal data protection training and workstation security.

Development project: Customers who hire Novicell consultants to deliver a development project. Novicell is responsible for the general personal data protection counselling, the consultant's general personal data protection training and workstation security.

Online marketing: Customers who hire Novicell consultants to carry out online marketing. Novicell is responsible for the consultant's general personal data protection training and workstation security.

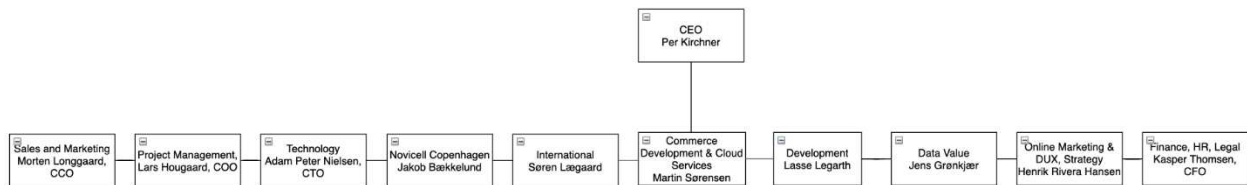
General control environment

The CEO is principal responsible for personal data protection and the Information Security Policy at Novicell. Novicell's Information Security Policy is the basis for data protection principles and guidelines. The Information Security Group is responsible for defining the principles and guidelines and revising the Information Security Policy. The CFO is responsible for developing and implementing the relevant controls that ensure compliance with the Information Security Policy. The Information Security Group reports to the CEO. The Information Security Group currently consists of:

- a. Kasper Thomsen, CFO
- b. Adam Nielsen, CTO
- c. Anne Mølgaard Brøndum, HR Legal Consultant
- d. Martin Sørensen, Head of Key Account Development and Cloud Services
- e. Jens Hagbard Grønkjær, Head of Data Value
- f. Emil Rasmussen, Web Architect.

The members of the Information Security Group are required to keep up to date with developments in information security and/or attend relevant training. The Information Security Group revises the Information Security Policy as well as the principles and guidelines yearly so that the policy complies with current legislation and contractual obligations. At the same time, the risk assessment is evaluated. Information security or personal data incidents are reported to the Information Security Group.

Organisation chart



Information Security Policy and organisational principles

To ensure coherence with the Information Security Policy and the organisation, the Information Security Group maintains the InfoSec Employee Manual that clearly communicates the Information Security Policy's principles and guidelines in everyday practical terms. Where applicable, the InfoSec Employee Manual is divided into areas specific for the service areas. The employee's department manager is responsible for communicating guidelines that ensure compliance with the Information Security Policy. Updates to the Information Security Policy and the InfoSec Employee Manual are announced to employees.

The Information Security Group has delegated the day-to-day operations to the Data Protection Team. The Data Protection Team is the single point of contact for both employees and customers regarding data protection and handling of personal data.

Employee safety

At Novicell, the HR activities related to information security are handled by the Finance, HR & Legal departments as well as by each employee's manager. The information security responsibility for each employee is determined within their job description and employment contract terms.

The employees receive training, guidelines and information regarding information security via their department manager who ensures that the level of training is relevant for the employees' duties, responsibilities and skills. This includes information about acute threats and relevant resources for questions regarding information security.

Each employee signs a confidentiality clause as part of the employment contract. In addition to this, each manager yearly confirms the implementation of the InfoSec Employee guide in their respective team. Each employee is responsible for complying with the Information Security Policy relevant for the individual's duties and reporting personal data incidents to the Data Protection Team.

Risk assessment

For the various Novicell service areas, a yearly risk assessment is carried out. The risks assessment describes which risks are identified and the controls in place to mitigate the risks. The CFO is principal responsible for the risk assessment, and the Information Security Group is responsible for carrying out the assessment yearly.

The risks for the various Novicell service areas vary as the responsibility for the different parts of the complete security lifecycle is spread across Novicell, its customers and its providers. The categories of personal data also vary with each customer, and, as a consequence, all personal data is handled as sensitive personal data. The InfoSec Employee Guide reflects this categorisation and the variability in service areas.

Control activities

Access control

Physical

Locations that contain production systems with personal data are only accessible to authorised personal with professional duties, and access is only granted with key card and code. The physical access control for production systems is the responsibility of the housing provider and the private cloud provider.

Logical

At all office, home and remote working locations, personal data is protected by workstation disk encryption and strong unique passwords. Password requirements are enforced on all Novicell user accounts.

Systems storing personal data or access to personal data are configured so only employees for whom it is relevant have access. All user accounts are individual; if this is not possible due to system constraints, multifactor authentication has been activated where possible.

Communication policies

In case of personal data incidents, customers are notified as soon as possible, no later than agreed in the DPA, via the issue management system agreed with the customer. If an issue management system is not implemented between the parties, email or phone can be used.

Communication with the customers' data subjects is the responsibility of the customers. In case the customers' data subjects contact Novicell, Novicell defers any requests to the specific customer.

Monitoring of personal data procedures and controls

Customer requests concerning their data subjects' right to erasure, right of access and right of data portability are logged and monitored by the Information Security Group.

Customer requests concerning their data subjects and controls as per the risk assessment are reported yearly by the Finance, HR & Legal departments. The report is presented to the Information Security Group.

Backup

Data is backed up at least daily or according to SLA agreements and in accordance with the risk assessment. The backup procedure is documented and is run automatically for the various systems. Backups for the production systems are also stored with the private cloud provider (Curanet), and they manage backup to a different geographic location than production data.

The Cloud Service department monitors the backup logs as part of the daily routine, and the status of the backup system is documented weekly.

At least once every year, a random selection of servers are chosen to validate the restore procedure.

Acquisition and maintenance of infrastructure

Networking

Company networks and devices are designed, deployed and operated in a manner so as to provide proper levels of protection for the data being accessed and transported.

The Cloud Services department is responsible for the company's network design and operation. Ongoing maintenance is documented in Novicell's case management system, and significant changes to network design and configurations are documented by Cloud Services.

Network documentation and patching status are reviewed at least yearly.

System software

System software is updated according to Novicell's procedures and vendors' guidelines. Each quarter, servers are reviewed for OS version and latest date of OS update and patch.

The Cloud Services department is responsible for maintaining system software and the control hereof.

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:

- g. Consider the consequences related to the protection of personal data when change requests are raised
- h. Consider/test new versions of systems at the implementation stage
- i. Handle the set-up and administration of own users of the solution in the production environment
- j. Handle the set-up and administration of users from Novicell ApS who provides assistance in the customer's environment
- k. Ensure that personal data are not included in support cases
- l. Consider how to ensure that personal data are anonymised when copied from production environments to test environments (typically necessary to enable a representative test of newly developed functionality before going live)
- m. Consider the need for having penetration tests carried out by a recognised security company to verify the security of the developed solution
- n. Inform Novicell ApS about changes in employees who have access to sites shared between the customer and Novicell ApS
- o. Ensure that any necessary DPIA is conducted and, based on this assessment, give Novicell ApS instructions for handling personal data
- p. Warrant that the purpose of the processing of personal data is lawful and fair and that Novicell ApS is only provided with the personal data necessary to fulfil the purpose
- q. Be responsible for ensuring that a legal basis for processing exists at the time of the transfer of the personal data to Novicell ApS – including that any consent is freely given, specific, informed, unambiguous as well as explicit, if required
- r. Warrant that the individuals to whom the personal data relate (the data subjects) have been sufficiently informed about the processing of their personal data
- s. Have the primary responsibility for giving Novicell ApS instructions about data processing and handle requests from data subjects regarding their rights
- t. Report any personal data breaches to the Danish Data Protection Agency.

4. Control objectives, control activity, tests and test results

Control objective A:

Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with in accordance with the data processing agreement entered into.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
A.1	<p>Written procedures are in place which include a requirement that personal data must only be processed when instructions to this effect are available.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Checked by way of inspection that formalised procedures are in place to ensure that personal data are only processed according to instructions.</p> <p>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.</p> <p>Checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
A.2	<p>The data processor only processes personal data stated in the instructions from the data controller.</p>	<p>Checked by way of inspection that Management ensures that personal data are only processed according to instructions.</p> <p>Checked by way of inspection of a sample of 6 personal data processing operations that these are conducted consistently with instructions.</p>	No exceptions noted.

Control objective A:

Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with in accordance with the data processing agreement entered into.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
A.3	The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions.	<p>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.</p> <p>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.</p> <p>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.</p>	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	<p>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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Checked by way of inspection that formalised procedures are in place to ensure establishment of the security measures agreed.</p> <p>Checked by way of inspection that procedures are up to date.</p> <p>Checked by way of inspection of a sample of 6 data processing agreements that the security measures agreed have been established.</p>	No exceptions noted.
B.2	<p>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.</p>	<p>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.</p> <p>Checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data.</p> <p>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.</p> <p>Checked by way of inspection that the data processor has implemented the security measures agreed with the data controller.</p>	No exceptions noted.
B.3	<p>For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.</p>	<p>Checked by way of inspection that antivirus software has been installed for the systems and databases used in the processing of personal data.</p> <p>Checked by way of inspection that antivirus software is up to date.</p>	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.	<p>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.</p> <p>Checked by way of inspection that the firewall has been configured in accordance with the relevant internal policy.</p>	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.	<p>Inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.</p> <p>Inspected network diagrams and other network documentation to ensure appropriate segmentation.</p>	No exceptions noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	<p>Checked by way of inspection that formalised procedures are in place for restricting users' access to personal data.</p> <p>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.</p> <p>Checked by way of inspection that the technical measures agreed support retaining the restriction in users' work-related access to personal data.</p> <p>Checked by way of inspection of a sample of 22 users' access to systems and databases that such access is restricted to the employees' work-related need.</p>	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.7	<p>System monitoring with an alarm feature has been established for the systems and databases used in the processing of personal data. This monitoring comprises:</p> <ul style="list-style-type: none"> • Netværksovervågning • Brugeradgange 	<p>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.</p> <p>Checked by way of inspection of alarms, these were followed up on and that the data controllers were informed thereof as appropriate.</p>	No exceptions noted.
B.8	<p>Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.</p>	<p>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.</p> <p>Checked by way of inspection that technological encryption solutions have been available and active throughout the assurance period.</p> <p>Checked by way of inspection that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.</p> <p>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.</p>	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	<p>Logging of the following matters has been established in systems, databases and networks:</p> <ul style="list-style-type: none"> • Activities performed by system administrators and others holding special rights • Security incidents comprising: <ul style="list-style-type: none"> ○ Changes in log set-ups, including disabling of logging ○ Changes in users' system rights ○ Failed attempts to log on to systems, databases or networks <p>Logon data are protected against manipulation and technical errors and are reviewed regularly.</p>	<p>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.</p> <p>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.</p> <p>Checked by way of inspection that user activity data collected in logs are protected against manipulation or deletion.</p> <p>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.</p> <p>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.</p>	<p>We have seen that the audit logging of the Domain Controller is not sufficient. No further exceptions noted.</p>
B.10	<p>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.</p>	<p>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.</p>	<p>No exceptions noted.</p>

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.	<p>Checked by way of inspection that formalised procedures are in place for regularly testing technical measures, including for performing vulnerability scans and penetration tests.</p> <p>Checked by way of inspection of samples that documentation confirms regular testing of the technical measures established.</p> <p>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.</p>	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.	<p>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.</p> <p>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.</p>	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.	<p>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.</p> <p>Checked by way of inspection of a sample of 10 employees' access to systems and databases that the user accesses granted have been authorised and that a work-related need exists.</p> <p>Checked by way of inspection of a sample of 12 resigned or dismissed employees that their access to systems and databases was deactivated or removed in a timely manner.</p> <p>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.</p>	No 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.	<p>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.</p> <p>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.</p>	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.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.	<p>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.</p> <p>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.</p>	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	<p>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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the information security policy should be updated.</p>	<p>Checked by way of inspection that an information security policy exists that Management has considered and approved within the past year.</p> <p>Checked by way of inspection of documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.</p>	No exceptions noted.
C.2	<p>Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.</p>	<p>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.</p> <p>Checked by way of inspection of a sample of 6 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.</p>	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	<p>The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant:</p> <ul style="list-style-type: none"> • References from former employers • Diplomas 	<p>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.</p> <p>Checked by way of inspection of a sample of 6 data processing agreements that the requirements therein for screening employees are covered by the data processor's screening procedures.</p> <p>Checked by way of inspection employees appointed during the assurance period that documentation states that the screening has comprised:</p> <ul style="list-style-type: none"> • References from former employers • Diplomas 	No exceptions noted.
C.4	<p>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.</p>	<p>Checked by way of inspection employees appointed during the assurance period that the relevant employees have signed a confidentiality agreement.</p> <p>Checked by way of inspection employees appointed during the assurance period that the relevant employees have been introduced to:</p> <ul style="list-style-type: none"> • The information security policy • Procedures for processing data and other relevant information. 	No exceptions noted.

Control objective C:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
C.5	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.	<p>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.</p> <p>Checked by way of inspection of 12 employees resigned or dismissed during the assurance period that rights have been deactivated or terminated and that assets have been returned.</p>	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.	<p>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.</p> <p>Checked by way of inspection of 12 employees resigned or dismissed during the assurance period that documentation confirms the continued validity of the confidentiality agreement and the general duty of confidentiality.</p>	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.	<p>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.</p> <p>Inspected documentation stating that all employees who have either access to or process personal data have completed the awareness training provided.</p>	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	<p>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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>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.</p> <p>Checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
D.2	<p>The following specific requirements have been agreed with respect to the data processor's storage periods and deletion routines:</p> <ul style="list-style-type: none"> • Upon agreement 	<p>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.</p> <p>Checked by way of inspection 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.</p>	<p>We have been informed that no terminations have required deletion of personal information.</p> <p>No exceptions noted.</p>
D.3	<p>Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been:</p> <ul style="list-style-type: none"> • Returned to the data controller and/or • Deleted if this is not in conflict with other legislation. 	<p>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.</p>	<p>We have been informed that no terminations have required deletion of personal information.</p> <p>No exceptions noted.</p>

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	<p>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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>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.</p> <p>Checked by way of inspection that procedures are up to date.</p> <p>Checked by way of inspection of a sample of 6 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.</p>	No exceptions noted.
E.2	<p>Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.</p>	<p>Checked by way of inspection that the data processor has a complete and updated list of processing activities stating localities, countries or regions.</p> <p>Checked by way of inspection of a sample of 6 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.</p>	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	<p>Written procedures are in place which include requirements for the data processor when using subprocessors, including requirements for sub-processing agreements and instructions.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Checked by way of inspection that formalised procedures are in place for using subprocessors, including requirements for subprocessing agreements and instructions.</p> <p>Checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
F.2	<p>The data processor only uses subprocessors to process personal data that have been specifically or generally approved by the data controller.</p>	<p>Checked by way of inspection that the data processor has a complete and updated list of subprocessors used.</p> <p>Checked by way of inspection of a sample of 4 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.</p>	No exceptions noted.
F.3	<p>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.</p>	<p>Checked by way of inspection that formalised procedures are in place for informing the data controller when changing the subprocessors used.</p> <p>Inspected documentation stating that the data controller was informed when changing the subprocessors used throughout the assurance period.</p>	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.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.	<p>Checked by way of inspection for existence of signed subprocessing agreements with subprocessors used, which are stated on the data processor's list.</p> <p>Checked by way of inspection of a sample of 4 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.</p>	No exceptions noted.
F.5	<p>The data processor has a list of approved subprocessors disclosing:</p> <ul style="list-style-type: none"> • Name • Company registration no. • Address • Description of the processing. 	<p>Checked by way of inspection that the data processor has a complete and updated list of subprocessors used and approved.</p> <p>Checked by way of inspection that, as a minimum, the list includes the required details about each subprocessor.</p>	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.6	Based on an updated risk assessment of each sub-processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the subprocessor.	<p>Checked by way of inspection that formalised procedures are in place for following up on processing activities at subprocessors and compliance with the sub-processing agreements.</p> <p>Checked by way of inspection of documentation that each subprocessor and the current processing activity at such processor are subjected to risk assessment.</p> <p>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.</p> <p>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.</p>	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	<p>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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>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.</p> <p>Checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
G.2	<p>The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.</p>	<p>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.</p>	<p>We have been informed that no transfers to third countries has occurred.</p> <p>No exceptions noted.</p>
G.3	<p>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.</p>	<p>Checked by way of inspection that formalised procedures are in place for ensuring a valid basis of transfer.</p> <p>Checked by way of inspection that procedures are up to date.</p> <p>Checked by way of inspection of a sample of 8 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.</p>	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	<p>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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>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.</p> <p>Checked by way of inspection that procedures are up to date.</p>	<p>No exceptions noted.</p>
H.2	<p>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.</p>	<p>Checked by way of inspection that the procedures in place for assisting the data controller include detailed procedures for:</p> <ul style="list-style-type: none"> • Handing out data • Correcting data • Deleting data • Restricting the processing of personal data • Providing information about the processing of personal data to data subjects. <p>Checked by way of inspection of documentation that the systems and databases used support the performance of the relevant detailed procedures.</p>	<p>We have been informed that there has not been any requests from data subjects.</p> <p>No exceptions noted.</p>

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	<p>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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>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.</p> <p>Checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
I.2	<p>The data processor has established the following controls to identify any personal data breaches:</p> <ul style="list-style-type: none"> • Awareness of employees • Monitoring of network traffic • Follow-up on logging of access to personal data 	<p>Checked by way of inspection that the data processor provides awareness training to the employees in identifying any personal data breaches.</p> <p>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.</p> <p>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.</p>	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	<p>If any personal data breach occurred, the data processor informed the data controller without undue delay and no later than 72 hours after having become aware of such personal data breach at the data processor or a subprocessor.</p>	<p>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.</p> <p>Made inquiries of the subprocessors as to whether they have identified any personal data breaches throughout the assurance period.</p> <p>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.</p> <p>Checked by way of inspection that all personal data breaches recorded at the data processor or the subprocessors have been communicated to the data controllers concerned without undue delay and no later than 72 hours after the data processor became aware of the personal data breach.</p>	<p>No exceptions noted.</p>
I.4	<p>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:</p> <ul style="list-style-type: none"> • The nature of the personal data breach • Probable consequences of the personal data breach • Measures taken or proposed to be taken to respond to the personal data breach. 	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>Checked by way of inspection of documentation that the procedures available support that measures are taken to respond to the personal data breach.</p>	<p>No exceptions noted.</p>

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.”

Kristian Kjærgaard Rasmussen

Kunde

Serienummer: 40b1a381-eb14-4aa1-9108-8d12b2625fd4

IP: 93.178.xxx.xxx

2023-11-03 11:54:03 UTC



Jesper Parsberg Madsen

PRICEWATERHOUSECOOPERS STATS-AUTORISERET

REVISIONSPARTNERSELSKAB CVR: 33771231

Statsautoriseret revisor

Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e

IP: 87.49.xxx.xxx

2023-11-03 12:38:50 UTC



Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstempelt med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan kan du sikre, at dokumentet er originalt

Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet

i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service <penneo@penneo.com>**. Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske signeringsbeviser indlejret i dokumentet ved at anvende Penneos validator på følgende websted: **<https://penneo.com/validator>**