Grant Thornton

Assurance report

Pronestor ApS

Independent auditor's ISAE 3000 assurance report with limited assurance on information security and measures pursuant to the data processing agreement with customers who have used the Pronestor ApS Planner, Visitor, Display, Insights and Workspace as of 21 October 2022

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

November 2022

Table of contents

Section 1: Pronestor ApS' description of processing activity for the supply of the Pronestor ApS' Planner, Visitor, Display, Insights and Workspace

The purpose of this description is to provide information for Pronestor ApS' customers and their stakeholders (including auditors) of compliance with the Data Processing Agreements.

Further, the purpose of this description, is to provide information of the processing security, technical and organisational measures, and responsibilities between the data controller (Pronestor's customers) and Pronestor ApS.

Nature of processing

Pronestor ApS' processing of personal data on behalf of the Data Controller primarily concerns hosting, supporting and managing these systems.

Personal data

Categories of data covered by the data processor agreement:
General personal data, including identification information such as name, initials, title, e-mail, phone number, organizational affiliations, profile picture (if users choose to upload a picture to the solution)

Categories of data subjects falling within the data processing agreement:

- Customers Authorised Users
- Contacts Persons of Customers

Instructions from the data controller

Pronestor does not commence the processing of customer data until an approved DPA stating the instructions from customer to Pronestor is signed by both parties. The DPA may be Pronestor standard DPA which is approved by default, or it may be a DPA of the customers. In case of the latter the DPA must be reviewed by Pronestor's DPO and signed by Pronestor's CEO in order to assure that instructions do not contravene the GDPR. If instructions do contravene the GDPR DPO will contact customer immediately.

Risk assessment

Pronestor has used a standard risk assessment tool to assess the potential impacts of all areas of business. The impact assessment model always addresses data protection (GDPR) as this is mandatory regardless of the risk in question.

Pronestor has identified the risks involved in the processing of personal data from the GDPR purpose of ensuring the rights and freedoms of natural persons.

Technical and organisational control measures

The organisation of IT-security is based upon Pronestor's IT-security policy and originates from ISO27001/2:2013.

Management of information security within the individual areas, are described below. Control objectives and controls, chosen by Pronestor, are also stated in the summary in section 4.

Information security policies

The information security policies in Pronestor are developed and maintained by the Pronestor Security Organisation and as a minimum on an annual basis approved by the management team as well.

The Security Policy is available on the intranet for all employees and new employees will be made aware of the policy as part of the onboarding process

Organization of information security

The management of Pronestor has defined and allocated all information security responsibilities and established an Information Security Organization.

The Information Security Framework implemented ensures that the responsibilities within the security organization are explicit and visible. Organizational duties are segregated in a way that functions with conflicting interests are distributed on different staff.

Mobile devices and teleworking

A mobile device policy and remote work procedure is in place to minimize the risk of portable workstations and remote work. Encryption and remote control of devices is in place. All staff goes through mandatory training in proper handling of information security when outside the office.

Human resource security

Prior to employment, Pronestor ensures that employees understand their responsibilities, and that they are suitable for the roles for which they are considered.

Depending on the role and responsibilities the candidate is to take on, there might be more gates for the candidate to pass before reaching the final phase and to be offered a contract. Finally, all employment contracts include a non-disclosure agreement covering information related to customer data, sales and marketing data, strategy, and other confidential business data.

We ensure that our employees receive continuous security training. This is done by sharing internal knowledge, relevant external courses, and certifications. All new employees must go through in an information security onboarding session.

Asset management

To ensure that all assets are handled with the proper attention ownership of assets is explicit. The ownership of all production related assets such as customer data, production environments and development environments fall on the CTO. Internal hardware and internal networks are the responsibility of the Internal Help Desk. Procedures are in place to ensure that inventory of assets are kept up to date and that hardware and mobile devices are disposed of securely to protect the confidentiality of Pronestor's customers.

Access control

Pronestor ensures that access to information and information processing facilities is limited. The Access control policy is based on a least privilege principle. Privileged access assignments may be segregated into organizational unit such as marketing, development, customer support or sales.

Access control includes enforced MFA (Multi Factor Authentication) and use of encrypted password managers.

User access is reviewed on a regular basis and reviews are recorded. Upon employee role changes or terminations, Pronestor handles off-boarding from central systems.

Cryptography

Pronestor employs encryption both at rest and in transit. Enryption in transit uses at least TLS 1.2. SSL 1.0, SSL 2.0, and SSL 3.0 are always disabled. All secrets such as user passwords used in systems are stored in a one-way hashed form using a salted hashing algorithm. Secrets are never stored in clear text.

Operations security

A policy on operational procedures has been established, and a change management workflow has been implemented to ensure the control of changes to the production environments and infrastructure.

Pronestor's Operations Manual contains information about essential areas of daily operations. Incidents are collected from various tools and sent to an alerting system that alerts relevant people. After an incident, a post-mortem is held.

Capacity monitoring is done on metrics from applications, databases and infrastructure. When thresholds are exceeded alerts are triggered to allow operations staff to scale as necessary. Development, testing and operational environments are completely separate from each other. Information saved in databases is backed up continuously and copied to the external storage.

Logs are stored in our log aggregation system to allow for correlation across systems and easy trouble shooting.

Communications security

Test, staging and production environments are segmented by separate networks and physically separated from the Pronestor office network. Changes to network infrastructure and firewalls are handled as peer reviewed terraform code changes in Pronestor's version control system Git.

Acquisition, development, and maintenance of systems

Pronestor information systems are designed and implemented according to the system development and security life cycle procedure. The process is structured and ensures a consistent high level of security and quality. Established change management workflow ensure that only relevant and necessary changes are made.

Supplier relationships

A process for assessing and managing risks associated with suppliers exists to protect Pronestor and their customers when using suppliers. Supplier relationships are monitored, reviewed, and audited on a regular basis to make sure suppliers adhere to both regulations and Pronestor's IT Security Policies.

Information security incident management

Procedures are in place to ensure a consistent and fast approach to information security incidents. The process describes communication both internally and externally. Regulatory requirements are part of these procedures to ensure that any breaches are not just handled promptly and effectively but are also reported to any relevant authorities. Post-mortems are an integral part of any incident to extract any learnings made during the incident.

Data protection officer
Pronestor is not in a category where the appointment of a DPO is mandatory. Pronestor has chosen to appoint a DPO to emphasize externally as well as internally that data protection is essential to Pronestor.

Records of processing activities
All Pronestor cloud services are standardized software, and all customer data is managed the same way. PII, data subject categories and categories of processing are alike from one customer to the next.

Records of processing activities are kept and maintained in Pronestor CRM from where they may be exported at any time. Information on data controllers and contact persons regarding GDPR are stores in CRM as well as instructions through the DPA. When the list is exported, information such as contact information for Pronestor's DPO is added manually.

Pronestor's technical and organizational measures are described in Pronestor's IT-Security Policy and maintained by the IT security organization.

Use of sub-data processors
All sub processors are chosen and evaluated according to Pronestor Outsourcing Procedure before an agreement and a sub-processor agreement is signed. Sub processors handling Customers PII are listed in the DPA and approved by data controller. If Pronestor wishes to add or change a sub processor Customers must be warned with a minimum of 2 months' notice according to DPA. DPO is responsible for providing contact information from CRM and informing customers accordingly.

Sub-processors are evaluated on a yearly basis and controlled through their external audits.

Transfer of personal data to third countries
Pronestor does not transfer personal data to third countries.

Assistance to the data controller for exercising the data subject's rights
Pronestor services are designed to give Customer full authority concerning their data. At any time, Customer may change user rights, delete users, and anonymize users. Pronestor recommends Customers to retain full control by using their AD to import and maintain users and users' rights in Pronestor services. In case AD is not used Customer may use the administrator interface to handle all user rights without Pronestor assistance.

Pronestor may assist Customer in performing these tasks if Customer places a ticket in Pronestor help-desk thereby documenting that Customer has instructed Pronestor to execute the changes in question.

Notification of personal data breach
The Incident Response Procedure describes how Pronestor handles incidents and states that in case PII is affected in an incident Pronestor DPO will be notified and immediately involved.

DPO will without any delay report incidents to the customers involved. DPO is responsible for maintaining an updated CRM and from there find contact information to notify customer(s) and report:

- Description of the PII breach
- How and which physical person may be at risk
- How Pronestor plans to handle the breach and minimize damage to physical persons
- How Pronestor will assist data controller in the event data controller needs to notify authorities

Complementary controls with the data controller

The controls are designed in such a way that some of the controls mentioned in this declaration must be complimented by controls on the data controller's side. The controls mentioned below are expected to be implemented and executed at and by the data controller for Pronestor to be able to fully comply with the controls in this report. The list of controls below should not be considered complete and exhaustive, and where deemed necessary, the data controller should add additional controls.

- Data controllers themselves are responsible for establishing a connection to the Pronestor servers. This includes the responsibility to have a functioning and adequate internet connection as well as tested and verified backup internet connections in case of connectivity issues.
- Data controllers themselves are responsible for administration of their own user accounts on application, system, and database level.
- Data controllers themselves are responsible for a regular audit of their own user accounts on application, system, and database level.
- Data controllers themselves are responsible for making sure created user accounts on application, system and database level are in sync with their employee roster.
- Should doubt arise on whether a user account has been compromised by for example laptop theft or similar, it is the responsibility of the data controller to inform Pronestor of the concern.
- Data controller's themselves are responsible for establishing a Continuity Plan to handle the data controller's company in case of emergency, major accidents, or disaster.

Section 2: Pronestor ApS' statement

The accompanying description has been prepared for Pronestor ApS' customers, who has entered a data processor agreement with Pronestor ApS related to the Pronestor ApS' Planner, Visitor, Display, Insights and Workspace, 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 omen the free movement of such data (hereinafter "the Regulation") have been complied with.

Pronestor ApS uses the following sub-supplier and sub-processor: Amazon AWS, Compaya and Flowmailer. This statement does not include control objectives and related controls at Pronestor ApS' sub-suppliers and sub-processors. Certain control objectives can only be achieved, if the sup-supplier's controls, which are assumed in the design of our controls, are appropriately designed and operationally efficient. The description does not include control activities performed by the sup-supplier.

Some of the control objectives stated in Pronestor ApS' description in Section 1 of the Pronestor ApS' Planner, Visitor, Display, Insights and Workspace, can only be achieved if the complementary controls with the customers have been appropriately designed and works efficiently with the controls with Pronestor ApS. The report does not include the appropriateness of the design and operating efficiency of these complementary controls.

Pronestor ApS confirms that:

a) The accompanying description, Section 1, fairly presents how Pronestor ApS has processed personal data on behalf of data controllers as of 21 October 2022. The criteria used in making this statement were that the accompanying description:

(i) Presents how Pronestor ApS' processes and controls related to data protection 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 the performed 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 safeguards 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 Pronestor ApS' Planner, Visitor, Display, Insights and Workspace 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) Does not omit or distort information relevant to the scope of the Pronestor ApS' Planner, Visitor, Display, Insights and Workspace 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 Pronestor ApS platform 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, in our opinion, suitable designed and implemented as of 21 October 2022, if relevant controls with sup-suppliers were operationally efficient and the customers have performed the complementary controls, assumed in the design of Pronestor ApS' controls as of 21 October 2022.

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.

c) Appropriate technical and organisational safeguards 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 General Data Protection Regulation.

Lyngby, 7 November 2022
Pronestor ApS

Karsten Johan Busck
CEO

Section 3: Independent auditor's assurance report with limited assurance on information security and measures pursuant to data processing agreements with customers as of 21 October 2022

To Pronestor ApS, their customers in the role of data controller and their auditors.

Scope

We were engaged to provide assurance about a) Pronestor ApS' Planner, Visitor, Display, Insights and Workspace in accordance with the data processing agreement with costumers as data controllers as of 21 October 2022 and b) about the design and implementation of controls related to the control objectives stated in the Description.

Pronestor ApS uses the following sub-suppliers and sub-processors: Amazon AWS, Compaya and Flowmailer. This statement does not include control objectives and related controls at Pronestor ApS' sub-suppliers and sub-processors. Certain control objectives in the description, can only be achieved, if the sup-supplier's controls, which are assumed in the design of Pronestor ApS' controls, are appropriately designed and operationally efficient together with the related controls with Pronestor ApS.

Some of the control objectives stated in Pronestor ApS' description in Section 1 of the Pronestor ApS platform, can only be achieved if the complementary controls with the customers have been appropriately designed and works effectively with the controls with Pronestor ApS. The report does not include the appropriateness of the design and operating effectiveness of these complementary controls.

We express limited assurance in our conclusion.

Pronestor ApS' responsibilities

Pronestor ApS is responsible for preparing the description and the accompanying statement, Section 2, including the completeness, accuracy, and the method of presentation of the Description and statement, providing the services covered by the Description; stating the control objectives; and designing, implementing 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 of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior and ethical requirements applicable to Denmark.

Grant Thornton 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.

Grant Thornton's responsibilities

Our responsibility is to express an opinion on Pronestor 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 have conducted our engagement in accordance with International Standard on Assurance Engagements 3000, "Assurance Engagements Other than Audits or Reviews of Historical Financial Information", and additional requirements under Danish audit regulation, to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are appropriately 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 Pronestor ApS' Planner, Visitor, Display, Insights and Workspace and about the design and operating effectiveness of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not appropriately designed or operating effectively. Our procedures have by analysis and inquiries, included assessment of the implementation of such 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 appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data processor and described in Section 1.

The scope of the actions we have taken, is less than the ones of an assurance report with reasonable assurance. Hence, the degree of certainty of our opinion is significantly less than the certainty that would have been accomplished, had the assurance report been issued with reasonable assurance.

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

Pronestor ApS' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Pronestor ApS' Planner, Visitor, Display, Insights and Workspace 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 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. During the audit work, we have not found any material aspects, that would lead us to form the opinion:

(a) that the Description does not fairly present Pronestor ApS' platform, as designed and implemented as of 21 October 2022 and

(b) that the controls related to the control objectives stated in the Description, not in all aspects were appropriately designed as of 21 October 2022, if controls with sup-suppliers were operationally efficient, and if customers who have used Pronestor ApS' platform, have designed, and implemented the complementary controls, assumed in the design of Pronestor ApS' control as per 21 October 2022.

Description of assessments of controls

The specific controls, (by analysis and requests) and the nature, timing, and results of those assessments are listed in Section 4.

Intended users and purpose

This report and the description of assessments of controls in Section 4 are intended only for data controllers who have used Pronestor ApS' Planner, Visitor, Display, Insights and Workspace, 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 Regulation have been complied with.

Copenhagen, 7 November 2022

Grant Thornton
State Authorised Public Accountants

Jacob Helly Juell-Hansen
State authorised public accountant

Basel Rimon Obari
Executive director, CISA, CISM

Section 4: Control objectives, control activities, assessment, and results hereof

We have conducted our engagement in accordance with ISAE 3000, assurance engagements other than audits or review of historical financial information.

Our assessment of the implementation has included the control objectives and attached controls, selected by management and which are stated in the control objectives A-I below. Our assessment has included the controls; we find necessary to establish limited assurance for compliance with the articles stated as of 21 October 2022.

This statement does not include control objectives and accompanying controls with Pronestor ApS' sub-supplier and sub-processor.

Further, controls performed at the data controller are not included in this statement.

We performed our assessment of controls at Pronestor ApS by the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at Pronestor ApS. The interviews have included questions about, how controls are performed.
Observation	Observing how controls are performed.
Inspection	Reading of documents and reports, including description of the performance of the control. This includes reading and assessment of reports and documents to evaluate whether the specific controls are designed in such a way, that they can the expected to be effective when implemented.
Re-performance	Re-performance of controls to verify that the control is working as assumed.

List of control objectives compared to GDPR-articles, ISO 27701, and ISO 27001/2

Below, control objectives are mapped against the articles in GDPR, ISO 27701 and ISO 270001/2.

Articles and points about main areas are written in bold.

Control activity	GDPR articles	ISO 27701	ISO 27001/2
A.1	5, 26, **28**, 29, 30, 32, 40, 41, 42, 48	8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, **8.2.2**	*New scope compared to ISO 27001/2*
A.2	**28**, 29, 48	8.5.5, 6.15.2.2, **6.15.2.2**	18.2.2
A.3	**28**	**8.2.4, 6.15.2.2**	18.2.2
B.1	31, **32**, 35, 36	**5.2.2**	4.2
B.2	**32,** 35, 36	**7.2.5, 5.4.1.2, 5.6.2**	6.1.2, 5.1, 8.2
B.3	**32**	**6.9.2.1**	**12.2.1**
B.4	28 stk. 3; litra e, **32; stk. 1**	**6.10.1.1, 6.10.1.2, 6.10.1.3**, 6.11.1.3	**13.1.2**, 13.1.3, 14.1.3, 14.2.1
B.5	32	6.6.1.2, 6.10.1.3	9.1.2, 13.1.3, 14.2.1
B.6	**32**	**6.6**	9.1.1, 9.2.5
B.7	**32**	**6.9.4**	12.4
B.8	**32**	**6.15.1.5**	18.1.5
B.9	**32**	**6.9.4**	12.4
B.10	**32**	**6.11.3**	14.3.1
B.11	**32**	**6.9.6.1**	12.6.1
B.12	28, **32**	**6.9.1.2, 8.4**	12.1.2
B.13	**32**	**6.6**	9.1.1
B.14	**32**	**7.4.9**	*New scope compared to ISO 27001/2*
C.1	**24**	**6.2**	5.1.1, 5.1.2
C.2	**32, 39**	**6.4.2.2, 6.15.2.1, 6.15.2.2**	7.2.2, 18.2.1,18.2.2
C.3	**39**	**6.4.1.1-2**	7.1.1-2
C.4	28, 30, **32, 39**	**6.10.2.3**, 6.15.1.1, 6.4.1.2	7.1.2, 13.2.3
C.5	**32**	**6.4.3.1, 6.8.2.5, 6.6.2.1**	7.3.1, 11.2.5, 8.3.1
C.6	**28,** 38	**6.4.3.1, 6.10.2.4**	7,3.1, 13.2.4
C.7	**32**	**5.5.3, 6.4.2.2**	7.2.2, 7.3
C.8	**38**	**6.3.1.1, 7.3.2**	6.1.1
C.9	6, 8, 9, 10, 15, 17, 18, 21, 28, **30**, 32, 44, 45, 46, 47, 48, 49	6.12.1.2, 6.15.1.1, 7.2.2, **7.2.8**, 7.5.1, 7.5.2, 7.5.3, 7.5.4, **8.2.6**, 8.4.2, 8.5.2, 8.5.6	*New scope compared to ISO 27001/2*
D.1	6, 11, **13, 14,** 32	**7.4.5**, **7.4.7**, 7.4.4	*New scope compared to ISO 27001/2*
D.2	6, 11, 13, 14, **32**	**7.4.5**, **7.4.7**, 7.4.4	*New scope compared to ISO 27001/2*
D.3	13, **14**	**7.4.7**, 7.4.4	*New scope compared to ISO 27001/2*
E.1	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*New scope compared to ISO 27001/2*

Control activity	GDPR articles	ISO 27701	ISO 27001/2
E.2	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*New scope compared to ISO 27001/2*
F.1	6, 8, 9, 10, 17, 18, 22, 24, 25, 28, **32,** 35, 40, 41, 42	5.2.1, **7.2.2**, **7.2.6**, 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7	15
F.2	**28**	**8.5.7**	15
F.3	**28**	**8.5.8**, 8.5.7	15
F.4	**33, 34**	**6.12.1.2**	15
F.5	**28**	**8.5.7**	15
F.6	**33, 34**	**6.12.2**	15.2.1-2
G.1	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, **8.5.1**, 8.5.2, 8.5.3	13.2.1, 13.2.2
H.1	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*New scope compared to ISO 27001/2*
H.2	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*New scope compared to ISO 27001/2*
I.1	**33, 34**	**6.13.1.1**	16.1.1-5
I.2	**33, 34**, 39	6.4.2.2, **6.13.1.5, 6.13.1.6**	16.1.5-6
I.3	**33, 34**	**6.13.1.4**	16.1.5
I.4	**33, 34**	**6.13.1.4,** 6.13.1.6	16.1.7

Control objective A - Instructions regarding processing of personal data

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	*Pronestor ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
A.1	Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inquired into whether formalised procedures exist to ensure that personal data are only processed according to instructions. We have inquired into whether procedures are updated and which updates, if any, were made. We have inspected the overview of formalised procedures and analysed whether this is sufficient.	No deviations noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	We have inquired into how management ensures that the processing of personal data is only processed according to instructions, and we have assessed the appropriateness of this. On a sample basis, we have inspected that the instructions in the data processing agreement is complied with.	No deviations 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.	We have inquired how the management is ensuring verification that personal data are not processed against the Regulation or other legislation. We have inquired into whether formalised procedures exist for informing the data controller in cases, where personal data processing is considered to be in violation with the legislation. We have assessed that it is likely that the data controller will be informed, if data processor considers the instructions to be in violation with legislation or data protection law other European Union or member state data protection provisions	No deviations noted.

Control objective B - Technical measures

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

No	*Pronestor ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
B.1	Written procedures exist which include a requirement that safeguards agreed are established for the processing of personal data in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inquired into whether formalised procedures exist to ensure the agreed technical measures. We have inquired into, whether procedures are updated and which updates, if any, were made. We have inspected the overview of formalised procedures and analysed whether this is sufficient.	No deviations 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 safeguards agreed with the data controller.	We have inquired whether the risk assessment is updated and includes the current processing of personal data. We have inquired into which technical measures have been implemented and how these ensures an appropriate level of security in compliance with the risk assessment. We have inspected that the data processor has implemented the technical measures, that are agreed with a data controller.	No deviations noted.
B.3	For the PC's used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.	We have inquired into whether antivirus software has been installed on the PCs used in the processing of personal data. We have inspected documentation that antivirus software has been installed and updated on a PC.	No deviations noted.
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	We have inquired into whether external access to systems and databases, used for personal data processing, only takes place through a firewall. We have inspected documentation that firewall is configured on the relevant unit.	No deviations noted.

Control objective B - Technical measures

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

No	*Pronestor ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	We have inquired whether internal networks have been segmented to ensure restricted access to systems and databases, used in the processing of personal data. We have inspected network diagrams and other network documentation to ensure appropriate segmentation.	No deviations noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	We have inquired into whether formalised procedures are in place for restricting users' access to personal data. We have inquired into whether procedures are in place for following up on users' access to personal data being consistent with their work-related needs. We have inspected documentation of periodic follow-up on user access rights. We have inspected the users with access to personal data is limited to employees with a work-related need.	No deviations noted.
B.7	For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.	We have inquired into whether systems and databases, used for personal data processing, are monitored, and equipped with alarms. We have inspected that there are system monitoring and alarms related here to.	No deviations noted.

No	Pronestor ApS' control activity	Grant Thornton's assessment (by analysis and inquiries)	Result of test
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	We have inquired into whether formalised procedures are established, to ensure that transmission of confidential and sensitive personal data through the internet is protected by an effective encryption, based on an approved algorithm. We have inquired into whether technological solutions for encryption have been available and activated throughout the entire period. We have inspected that the setup of transmission paths is effective. We have inquired into whether unencrypted transmissions of sensitive and confidential personal data have been performed during the audit period, and whether the data controllers have been duly informed hereof.	We have been informed, that no unencrypted transmissions have been made within the last year, wherefore we have not been able to test the implementation of this part of the control. No deviations noted.
B.9	Logging has been established in systems, databases, and networks. Logon data are protected against manipulation and technical errors and are reviewed regularly.	We have inquired into whether policies have been established for setting up the logging of user activities in systems, databases and networks used for personal data processing, including review and follow-up on logs. We have inquired into whether user activities in systems, databases, and networks, used for personal data processing have been configured and activated. We have inquired into whether information about user activities in logs are protected against manipulation and deletion. We have inspected a sample of an extract of user activity logging.	No deviations noted.

No	Pronestor ApS' control activity	Grant Thornton's assessment (by analysis and inquiries)	Result of test
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.	We have inquired into whether formalised procedures are established for personal data used in development, testing or similar activity, ensuring that the use solely is performed in pseudonymized or anonymized form. We have inquired into how test data are anonymized and how data are being generated.	No deviations noted.
B.11	The technical measures established are tested on a regular basis in penetration tests.	We have inquired into whether formalised procedures exist for regularly testing of technical measures, including performing penetration tests. We have inspected that a penetration test has been performed. We have inquired into whether deviations are followed-up upon.	No deviations noted.
B.12	Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches.	We have inquired into whether formalised procedures exist for handling changes to systems, databases, and networks, including handling of relevant updates, patches, and security patches. We have, by sample test, inspected a change to establish that the procedure has been followed. Including that changes have been tested, approved and that Segregation of Duties are implemented in the process.	No deviations noted.
B.13	A formalised procedure is in place for granting and removing users' access to personal data.	We have inquired into whether formalised procedures exist for granting and removing users' access to systems for personal data processing. We have inquired whether there has been any new or terminated employees after the procedure was designed.	We have been informed that there has been no new or terminated employees after the procedure was designed, wherefore we are not able to test the implementation of the control. No deviations noted.

No	Pronestor ApS' control activity	Grant Thornton's assessment (by analysis and inquiries)	Result of test
B.14	Access to systems and databases processing personal data that involve a high risk for the data subjects are as a minimum only accessed by using two-factor authentication.	We have inquired into whether formalised procedures exist, ensuring that two-factor authentication is used when relevant. We have inspected that user access to process personal data, that involves high-risk for the registered, is only accessed through two-factor authentication.	No deviations noted.

Control objective C - Organisational measures

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

No	Pronestor ApS' control activity	Grant Thornton's assessment (by analysis and inquiries)	Result of test
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 IT security policy is based on the risk assessment performed. Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.	We have inquired into whether an information security policy exists, that management has assessed and approved within the past year. We have inspected that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No deviations noted.
C.2	Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.	We have inspected a sample of a typical data processing agreement, to establish whether the requirements are covered by the requirements of security measures and processing security in the information security policies	No deviations noted.
C.3	The employees of the data processor are screened as part of the employment process.	We have inspected that formalised procedures exist to ensure that the data processor's employees are screened as part of the employment process. We have inquired whether there have been any new employees after the procedure was designed.	We have been informed that there have been no new employees after the procedure was designed, wherefore we are not able to test the implementation of the control. No deviations noted.

Control objective C - Organisational measures

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

No	*Pronestor ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
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.	We have inspected the template for confidentiality agreements with employees, as part of the employment contract. We have inquired whether there have been any new employees after the procedure was designed.	We have been informed that there have been no new employees after the procedure was designed, wherefore we are not able to test the implementation of the control. No deviations noted.
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.	We have inquired into whether procedures exist to ensure that terminated employees' rights are inactivated or deleted upon resignation, and that assets such as access cards, computers, mobile phones etcetera, are returned. We have inquired whether any employees have been terminated after the procedure was designed.	We have been informed that there have been no terminated employees after the procedure was designed, wherefore we are not able to test the implementation of the control. No deviations 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.	We have inquired into whether formalised procedures exist to ensure that resigned or dismissed employees are made aware of the continued validity of the non-disclosure agreement and the general duty of confidentiality. We have inquired whether any employees have been terminated after the procedure was designed.	We have been informed that there have been no terminated employees after the procedure was designed, wherefore we are not able to test the implementation of the control. No deviations noted.

Control objective C - Organisational measures

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

No	*Pronestor ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
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.	We have inquired into whether the data processor provides awareness training for the employees, including general IT-security and GDPR. We have inspected documentation for the content of the awareness training includes GDPR and general IT-security.	No deviations noted.
C.8	The processor has assessed the need for a DPO and has ensured that the DPO has the adequate professional competence to perform their tasks and are involved in relevant areas.	We have inquired whether the company has assessed the need for a DPO.	No deviations noted.
C.9	The processor keeps a record of categories of processing activities for each data controller. Regularly – and at least annually – an assessment is made of whether the record of categories of processing activities for each controller should be updated.	We have inquired about the list, and we have inspected that the list contains relevant information. We have inquired into whether the list has been updated within the last year, or in case of relevant events. We have inquired into whether the list has been approved by the data processor's management.	No deviations noted.

Control objective D - Return and deletion of personal data

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	*Pronestor ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
D.1	Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inquired into whether formalised procedures or policies are in place for storing or deleting of personal data in accordance with the agreement with the data controller. We have inquired into whether procedures and policies are updated, and if so, which updates have been made. We have inspected the list of written policies and assessed whether this appears to be updated and adequate according to the agreed storing and deletion of personal data.	No deviations noted.
D.2	Specific requirements have been agreed with respect to the data processor's storage periods and deletion routines.	We have inquired into whether the existing procedures or agreements of storing, and deletion contains the specific requirements for the data processor's storage periods and deletion routines. We have, by sample test, inspected discontinued data processing agreements and inspected that data have been deleted in accordance with the data processing agreement.	No deviations noted.
D.3	Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been: • Returned to the data controller; and/or • Deleted if this is not in conflict with other legislation.	We have inquired if there are formal procedures in place for processing the data controller's data upon termination of the processing of personal data. We have, by sample test inspected discontinued data processing agreements and inspected that data has been deleted in accordance with the data processing agreement.	No deviations noted.

Control objective E – Storage of personal data

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	*Pronestor ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
E.1	Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inquired into whether formalised procedures or policies exist that storage and processing of personal data are only performed in accordance with the data processing agreements. We have inquired into whether the procedures have been assessed on a regular basis.	No deviations 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.	We have inquired into whether the data processor has a complete and updated list of processing activities stating localities, countries, or regions. We have inspected that a data processing agreement includes an overview of data processing activities and that storage of personal data only takes place in the localities mentioned in the data processing agreement – or otherwise is approved by the data controller.	No deviations noted.

Control objective F – Use of sub-processors

Procedures and controls are complied with to ensure that only approved sub-data processors 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	*Pronestor ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
F.1	Written procedures exist which include requirements for the data processor when using sub-data processors, including requirements for sub-data processing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inquired into whether formalised procedures are in place for using sub-data processors, including requirements for sub-data processing agreements and instructions. We have inquired into when procedures are being updated and which updates have been performed. We have inspected the list of written procedures and assessed whether this appears to be updated and adequate in relation to the use of sub data processors.	No deviations noted.
F.2	The data processor only uses sub-data processors to process personal data that have been specifically or generally approved by the data controller.	We have inspected that the data processor has a complete and updated list of sub-data processors used. We have, by sample test, inspected that documentation exist that the processing of data by the sub data processor is stated in the data processing agreement – or otherwise as approved by the data controller (specifically or indirectly).	No deviations noted.
F.3	When changing the generally approved sub-data processors 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 sub-data processors used, this has been approved by the data controller.	We have inquired into whether formalised procedures are in place for informing the data controller when changing the sub-data processors used. We have inspected that the data controllers have been informed about changes in the approved sub-data processors used.	No deviations noted.
F.4	The data processor has subjected the sub-data processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	We have inquired whether there are signed sub-data processor agreements with sub-data processors from the data processors overview. We have inspected a sample of the existence of signed sub-data processing agreements with sub-data processors used, which are stated on the data processor's list.	No deviations noted.

Control objective F – Use of sub-processors

Procedures and controls are complied with to ensure that only approved sub-data processors 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	*Pronestor ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
F.5	The data processor has a list of approved sub-data processors.	We have inspected that the data processor has a complete and updated list of sub-data processors used and approved.	No deviations noted.
F.6	Based on an updated risk assessment of each sub-data 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 sub-data processor.	We have inquired into whether formalised procedures are in place for following up on processing activities at sub-data processors and compliance with the sub-data processing agreements. We have inspected documentation that a risk assessment of the sub data processor has been performed, and that an ongoing follow up on the sub-data controller has been established in accordance with the risk assessment.	No deviations noted.

Control objective G – Transfer of personal data to third countries

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	*Pronestor ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
G.1	Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have, by sample test inspected, that data processing agreements describes the procedure for transfer to third countries. We have inquired into whether personal data are transferred to third countries, and we have inspected the list of data locations.	Not relevant, since we have been informed, that personal data are not transferred to third countries or international organisations, and we find this probable, based on our tests. No deviations noted.

Control objective H – Rights of the data subjects

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	*Pronestor ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
H.1	Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inquired whether formalised procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects. We have inquired whether procedures are updated and if so, which updates have been made. We have inspected the overview of written procedures and assessed whether they appear updated and adequate in relation to assistance to the data controller.	No deviations noted.
H.2	The data processor has established procedures as far as this was agreed that 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.	We have inquired into whether there is a procedure in place for assisting the data controller. We have assessed that it is likely that the systems and databases used, support the performance of the mentioned detailed procedures.	No deviations noted.

Control objective I – Managing personal data breaches

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	*Pronestor ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
I.1	Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inquired into whether formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. We have inquired into whether procedures are updated and which updates, if any, have been performed. We have inspected list of written procedures and assessed whether these appear to be updated and adequate in relation to the managing of personal data breaches.	No deviations noted.
I.2	The data processor has established the following controls to identify any personal data breaches: • Awareness of employees • Monitoring of network traffic	We have inquired into which control measures have been established to ensure that the company detects personal data breaches on time. We have inspected that the network traffic is monitored, and that the data processor offers awareness training to the employees.	No deviations noted.
I.3	If any personal data breach occurred, the data processor informed the data controller without undue delay after having become aware of such personal data breach at the data processor or a sub-data processor.	We have inspected that the data processor has an overview of security incidents, disclosing whether the individual incidents involved a personal data breach. We have inspected that the data processor has included possible personal data breaches with sup-data processors, in the data controller's list of security breaches. We have inquired into whether all recorded personal data breaches with the data processor or sub-data processors, have been communicated to the concerned data controllers without unnecessary delay after the data processor has become aware of such breach.	No deviations noted.

Control objective I – Managing personal data breaches

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	*Pronestor ApS' control activity*	*Grant Thornton's assessment (by analysis and inquiries)*	*Result of test*
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency.	We have inquired whether the procedures in place for informing the data controllers in the event of any personal data breach include detailed procedures for: • Describing the nature of the personal data breach • Describing the probable consequences of the personal data breach • Describing measures taken or proposed to be taken to respond to the personal data breach. We have assessed whether it is likely that procedures exist to support that measures are taken to manage the personal data breach.	No deviations noted.

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."

Karsten Johan Busck
Underskriver 1
Serienummer: PID:9208-2002-2-989140174535
IP: 82.192.xxx.xxx
2022-11-08 12:11:58 UTC
NEM ID

Basel Obari
Underskriver 2
Serienummer: CVR:34209936-RID:99589866
IP: 82.192.xxx.xxx
2022-11-08 12:14:55 UTC
NEM ID

Jacob Helly Juell-Hansen
Underskriver 3
Serienummer: CVR:34209936-RID:50904197
IP: 83.92.xxx.xxx
2022-11-09 12:32:40 UTC
NEM ID