Assurance report

XMedicus Systems ApS

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with customers that have used XMedicus EPJ per 5 December 2023

December 2023

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

Table of Contents

Section 1: XMedicus Systems ApS' statement

The accompanying description has been prepared for customers who have signed a data processing agreement with XMedicus Systems ApS and who have a sufficient understanding to consider the description along with other information, including information about controls, which the data controller himself has performed, in assessing whether the requirements in EU's regulation on protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter the General Data Protection Regulation) have been complied with.

XMedicus Systems ApS uses sub-processors KMD A/S and OnlineCity.IO ApS. This report does not include control objectives and affiliated controls with XMedicus Systems ApS' subprocessors. Certain control objectives in the description can only be achieved, if the subprocessor's controls, assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities, performed by subprocessors.

Some of the control objectives stated in XMedicus Systems ApS' description in Section 3 of XMedicus EPJ can only be achieved if the complementary controls with the customers are appropriately designed and works effectively with the controls with XMedicus Systems ApS. This report does not include the appropriateness of the design and the operating effectiveness of these complementary controls.

XMedicus Systems ApS confirms that:

a) The accompanying description, Section 3, fairly presents XMedicus EPJ which has processed personal data for data controllers subject to the Regulation per 5 December 2023. The criteria used in making this statement were that the accompanying description:

   (i) Presents how XMedicus EPJ 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 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 XMedicus EPJ 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 XMedicus EPJ 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 XMedicus EPJ 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 view, suitably designed and implemented per 5 December 2023, if relevant controls with subprocessors were operationally effective and data controller has performed the complementary controls, assumed in the design of XMedicus Systems ApS' controls as of 5 December 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; and

(ii) The identified controls would, if implemented 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 Regulation.

Søborg, 12 December 2023
XMedicus Systems ApS

Harald Madsen	Mikkel Kruse Johnsen
CFO	CEO

Section 2: Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to XMedicus Systems ApS' data processing agreement with customers

To: XMedicus Systems ApS, their customers, and their auditors

Scope

We were engaged to provide assurance about a) XMedicus Systems ApS' description, Section 3, of XMedicus EPJ in accordance with the data processing agreement with costumers per 5 December 2023 and about b) the design and implementation of controls related to the control objectives stated in the Description.

XMedicus Systems ApS uses the following subprocessors: KMD A/S and OnlineCity.IO ApS. This statement does not include control objectives and related controls at XMedicus Systems ApS' subprocessors. Certain control objectives in the description can only be achieved if the sub-processor's controls, assumed in the design of our controls, are appropriately designed, and operating effectively. The description does not include control activities performed by sub-processors.

Some of the control objectives stated in XMedicus Systems ApS' description in Section 3 of XMedicus EPJ, can only be achieved if the complementary controls with the customers have been appropriately designed and operating effectively with the controls with XMedicus Systems ApS. The report does not include the appropriateness of the design and operational effectiveness of these complementary controls.

We express reasonable assurance in our conclusion.

XMedicus Systems ApS' responsibilities

XMedicus Systems ApS is responsible for: preparing the Description and the accompanying statement, Section 1, 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; designing and implementing controls to achieve the stated control objectives.

Grant Thornton'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 behaviour and ethical requirements applicable to Denmark.

Grant Thornton is subject to the International Standard on Quality Control (ISQM 1) and accordingly uses and maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on XMedicus Systems ApS' Description and on the design and implementation of controls related to the control objectives stated in that Description, based on our procedures.

We 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 implemented.

An assurance engagement to report on the Description, design, and implementation of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of its XMedicus EPJ and about the design and implementation 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. Our procedures included testing the implementation 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 appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data processor and described in Section 1.

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

Limitations of controls at a data processor

XMedicus Systems ApS' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of XMedicus EPJ 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 1. In our opinion, in all material respects:

(a) The Description fairly presents XMedicus EPJ as designed and implemented per 5 December 2023; and

(b) The controls related to the control objectives stated in the Description were appropriately designed as pr. 5 December 2023; to obtain reasonable assurance that the control objectives stated in the Description would be obtained if controls with sub-processor were operating effectively and if data controller has designed and implemented the complementary controls, assumed in the design of XMedicus Systems ApS controls during as pr. 5 December 2023.

Description of tests 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 XMedicus Systems ApS' XMedicus EPJ 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.

Søborg, 12 December 2023

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Isabella Ørgaard Jensen
Director, CISA

Section 3: XMedicus Systems ApS' description of processing activity for the supply of XMedicus EPJ

The purpose of this description is to provide information to XMedicus Systems ApS' customers and their stakeholders (including auditors) about compliance with the data processing agreements with customers.

In addition, the purpose of this description is to provide information about processing security, technical and organizational measures, and responsibilities between data controllers (our customers) and XMedicus Systems ApS.

The nature of the data processed

The processing of personal data on behalf of the data controller is carried out primarily by XMedicus Systems ApS:

1. Stores data on dedicated servers and electronic storage devices,
2. Processes personal data according to specific instructions from the data controller in order to assist the data controller with data extraction, necessary changes, error corrections, conversion of data and deletion of data,
3. Facilitates the exchange of messages, referrals, epicrisis, invoices and the like between the data controller and the data subjects as well as authorities and other stakeholders,
4. Provides user support for the data controller's staff,
5. Provides technical support,
6. Ensures the data controller's access to data,
7. Makes a backup of the data controller's data.

Categories of personal information covered by the Data Processing Agreement

- General personal data, including identification information such as name and address, age, family relationship, e-mail address, telephone number, customer ID, personal doctor, payment information, insurance conditions and authorization number.
- Special categories of personal data, including, genetic data, sexual relationships and orientation and health information.
- Other sensitive information, such as social security numbers and special health information.

The following categories of registered persons are covered by the data processing agreement:

- The data controller's patients (children and adults)
- Employees of the data controller

Instructions from the data controller

To the extent that XMedicus Systems ApS' employees receive instructions from the data controller, which are clearly within the instructions, Annex C to the data processing agreement, e.g. user support, processing is carried out without further assessment or documentation.

To the extent that XMedicus Systems ApS' employees receive instructions from the data controller, which include processing as described in Section 2 above, e.g. data extraction, or other instructions that do not immediately appear in the data processing agreement, the individual employee assesses whether there may be doubts about the legality.

XMedicus Systems ApS' employees go through internal training and awareness training to ensure the necessary competence to assess the legality of instructions received from the data controllers. There is also internal documentation in the form of "procedure for handling data processing agreements" which can support the employees in the assessment.

To the extent that the employee considers that there may be doubts about the legality, the DPO is requested by XMedicus Systems ApS to carry out an assessment of the legality.

As part of this assessment, both the instructions received, and the assessment are documented.

Risk assessment

Concrete risk assessments of treatment activities have been carried out. All risk assessments are documented in an ISMS system.

There have not been situations where we have been requested to assist data controllers in carrying out an impact analysis.

Technical and organizational control measures

We implement the following technical and organizational measures to protect personal data, as follows:

Organizational security measures:

- Policies and procedures

- Internal teaching and awareness training
  - Own developed courses based on the company's core business area
  - Teaching and awareness training are documented in the LMS platform Eloomi

- Knowledge sharing by email and at Friday meetings
- ISAE 3000 declaration
- Increased cooperation and purchase of services within IT security
- Created a full-time compliance function
- DPO

Technical security measures:

- VPN connection to access the servers and database
  - Two-factor
  - Issuance of certificates

- DNSSEC on the email server domain
- The authenticity mark against phishing on the mail server – DMARC, DKIM and SPF
- Encryption on the e-mail server – TLS
- Antivirus in the form of Windows Defender on Windows machines
- Zabbix network scan

- Firewalls
  - FirewallD (Front end) on Linux servers
    - IPRange (Back end)

- Continuous updating of the EHR system
- Network segmentation
- BitLock encryption on PC
- Physical
- Alarms in the offices

- Locked outer door 24/7

- Penta - physical access restriction
  - Image scanner must be registered with the guard before it is activated.
  - Technical chief must confirm and order access to the employee in question on Penta's internal page.
  - Access card
  - Key to server cabinet
  - Locked building

- Backup once a day
- Uses Shodan to scan servers for anomalies.
- Automatic update of the Linux servers every night, running the update packages including the patches from Red Hat.
- The servers have mounted partitions, which the technical chief controls through a script.

Data protection officer (DPO)

Based on the nature and extent of the data recorded, it is our assessment that we must have a DPO.

It is based on the fact that the processing activity includes regular processing of sensitive information in the form of CPR numbers.

The DPO is selected and the person in question is independent of the management and recognized in the organization.

Through various courses, conferences, and online access to information material, we ensure that the person in question has the right qualifications for the position.

Use of subprocessors

Choice of subprocessors
Prior to signing agreements with subprocessors, audit statements are obtained and reviewed. To the extent deemed necessary, additional information is obtained from the subprocessor prior to entering into an agreement.

In addition, the subprocessor agreement is reviewed to ensure that it does not conflict with applicable legislation and the data processing agreements entered into by XMedicus Systems ApS.

The data controller's rights are secured through subprocessor agreements with the subprocessor.

Ongoing supervision of subprocessors
Supervision of the subprocessors is carried out annually and is based on the subprocessor's audit statements. To the extent deemed necessary, additional information is obtained from the subprocessor.

New subprocessors
In case of change or addition of subprocessors, the data controllers are informed of the change per e-mail, which contains the necessary information about the new subprocessor as well as a text that makes it clear that the data controller has 30 days to object to the use of the subprocessor in question.

XMedicus Systems ApS has prepared and continuously maintains a list of all data controllers and their respective contact persons.

XMedicus Systems ApS has not, within the past two years, prior to the date of this system description, changed or added any subprocessors.

Transfer of personal data
No personal data is being transferred to third countries. As of 28 June 2021, Great Britain is approved by the EU Commission as a safe third country where there is no need for a transfer basis.

The rights of the data subjects
It appears from point 9 of the data processing agreement, how XMedicus Systems ApS assist the data controller in fulfilling the data controller's obligation to respond to requests for the exercise of data subjects' rights as laid down in Chapter III of the Data Protection Regulation.

Handling personal data security breaches
XMedicus Systems ApS ensures that personal data security breaches are identified by:

- Ongoing training of employees through various awareness courses, including courses with a focus on personal data security and security for the registered
- Employees are trained to detect breaches.
- Possible breaches are entered into an event log document, which weekly compliance reviews.
- Weekly meetings are held with all employees, reviewing relevant incidents and possible situations.
- Internal policies and procedures are in place to identify and report security breaches.
- XMedicus Systems ApS CTO has established alarms monitoring and a log on relevant systems, and in the event of deviations, a report is made to the CTO, who assesses which measures must be carried out.
- If a significant breach is identified, the data controllers are informed within 24 hours of the discovery of the breach.

List
In our compliance software, there is a list of all customers (data controllers)

For each data controller is registered:

- Copy of data processing agreement
- Treatment activities
- Contact information for representatives of the data controller

The information is maintained on an ongoing basis and an annual review of the register is carried out.

The general description of technical and organizational security measures can be found in the procedure "A2 Information Policy XM", which is regularly updated.

Reference is also made to section 4, where the specific control activities are described.

Complementary user entity controls, performed by the data controllers

The data controllers have the following obligations:

- to ensure that the personal data is up to date,
- to make sure that the instruction is legal in relation to the personal data law regulation applicable at any time,
- that the instructions are appropriate in relation to this data processing agreement and the main service,
- to ensure that the data controller's users are up to date,
- to ensure that the necessary authorization for processing is present,
- to comply with the obligation to provide information to those registered about the exercise of their rights,
- to verify the identity of the data subjects who wish to exercise their rights.

Section 4: Control objectives, controls, tests, and results hereof

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

Our test 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 test has included the controls, we find necessary to establish reasonable assurance for compliance with the articles stated per 5 December 2023.

Our statement, does not apply to controls, performed at XMedicus Systems ApS' sub-processors.

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

We performed our test of controls at XMedicus Systems ApS by the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at XMedicus Systems ApS. The interviews have included questions about, how controls are performed.
Observation	Observing how controls are performed.
Inspection	Review and evaluation of policies, procedures and documentation concerning the performance of controls. This includes reading and assessment of reports and documents in order to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented. Further, it is assessed whether controls are monitored and controlled adequately and with suitable intervals.
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 27001/2:2013
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*
B.15	**32**	**6.8**	11.1.1-6
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*
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

Control activity	GDPR articles	ISO 27701	ISO 27001/2:2013
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
G.2	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1,** 7.5.2, 7.5.3, 7.5.4, **8.4.2,** 8.5.2, 8.5.3	13.2.1
G.3	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
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.	*XMedicus Systems ApS' control activity*	*Tests performed by Grant Thornton*	*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 inspected that formalised procedures exist to ensure that personal data are only processed according to instructions. We have inspected 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. We have inspected that procedures are up to date.	No deviations noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	We have inspected that management ensures that personal data are only processed according to instructions. We have, by sample test, inspected that personal data processing operations are conducted consistently with instructions.	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 inspected that formalised procedures exist ensuring verification that personal data are not processed against the Regulation or other legislation. We have inspected that procedures are in place for informing the data controller of cases where the processing of personal data is evaluated to be against legislation. We have inquired whether the data processor has received instructions which, in the data processor's opinion, infringes the data protection regulation or data protection provisions in other EU law or the national law of the member states.	We have been informed that the data processor has not received instructions which, in the data processor's opinion, infringes the data protection regulation or data protection provisions in other EU law or the national law of the member states, wherefore we have not tested the implementation of the control. 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.	*XMedicus Systems ApS' control activity*	*Tests performed by Grant Thornton*	*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 inspected the information security policy and that it contains relevant requirements for security measures related to the processing of personal data. We have inspected documentation that the information security policy has been reviewed and updated.	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 inspected the risk assessment and that it contains relevant risks associated with the processing of personal data. We have inspected documentation that risk assessments have been prepared for the significant subprocessors. We have inspected documentation that the risk assessment has been reviewed and updated.	No deviations noted.
B.3	For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.	We have inspected documentation to ensure that antivirus is active and up to date on the most recently employed employee's PC, which is used for processing personal data.	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 inspected that external access to systems and databases used for processing personal data only takes place through a firewall. We have inspected firewall rules for the various networks. We have inspected that a firewall is set up and that it is updated.	No deviations noted.
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 into 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.

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.	*XMedicus Systems ApS' control activity*	*Tests performed by Grant Thornton*	*Result of test*
B.6	Access to personal data is isolated to users with a work-related need for such access.	We have inspected the procedure for granting and terminating user access to personal data and it has been reviewed and approved by management. We have inspected documentation that users' access to systems and databases is limited to the employees' work-related needs.	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 inspected the system monitoring and alerting procedure and it has been reviewed and approved by management. We have inspected documentation that technical measures have been implemented in relation to system monitoring and alarming. We have inspected documentation of how the latest alarm was received and handled.	No deviations noted.
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	We have inspected documentation to ensure that effective encryption is used when transmitting and processing personal data. We have inspected documentation to ensure that drives used for processing personal data are automatically set up with encryption upon creation.	No deviations noted.
B.9	Logging has been established in systems, databases, and networks. Log data are protected against manipulation.	We have inspected that logging of user activities in systems used for the processing and transmission of personal data is configured and activated. We have inspected that gathered information about user activity in logs is protected from manipulation and deletion.	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.	*XMedicus Systems ApS' control activity*	*Tests performed by Grant Thornton*	*Result of test*
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	We have inspected documentation that software for vulnerability scans has been implemented. We have inspected documentation for handling the latest potential vulnerability.	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 inspected the procedure for changes to systems, databases, and networks and that it has been reviewed and approved by management. We have inspected documentation to ensure that the latest implemented change has followed the procedure.	No deviations noted.
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	We have inspected the procedure for granting and terminating user access to personal data and that it has been reviewed and approved by management. We have inspected documentation that the most recent employee has been given access to systems based on a work-related need. We have inquired whether there have been any resignations within the past year, with access to personal data. We have inspected documentation that monthly controls have been implemented to review user access.	We have been informed that no employees with access to the system where personal data is processed for the data controllers have resigned, wherefore we have not been able to test the implementation of the control related to removing user accesses. No deviations 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.	We have inspected documentation that two-factor authentication has been implemented when processing personal data.	No deviations noted.
B.15	Physical access safeguards 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.	We have inspected that appropriate physical access security has been established for offices and server room.	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.	*XMedicus Systems ApS' control activity*	*Test performed by Grant Thornton*	*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 inspected the information security policy that management has reviewed and approved within the past year. We have inspected documentation that the information security policy has been communicated to relevant 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 the information security policy. We have inspected documentation of management's assessment that the information security policy generally meets the requirements for safeguards and the security of processing in the data processing agreements entered.	No deviations noted.
C.3	The employees of the data processor are screened as part of the employment process.	We have inspected that there are formalized procedures that ensure verification of the data processor's employees in connection with employment. We have inspected documentation that the most recent employee has been screened according to the procedure.	No deviations noted.
C.4	Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.	We have inspected that the most recently hired employee has signed a confidentiality agreement. We have inspected that the most recently hired employee has been introduced to the information security policy and procedures relevant to the employee's duties.	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.	*XMedicus Systems ApS' control activity*	*Test performed by Grant Thornton*	*Result of test*
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 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. We have, by sample test, inspected that rights have been deactivated or terminated and that assets have been returned for employees resigned or dismissed.	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 inspected that formalised procedures exist to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality. We have, by sample test, inspected that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality for employees resigned or dismissed.	No deviations 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.	We have inspected that the data processor offers awareness training to employees covering general IT security and processing security in relation to personal data. We have inspected documentation that all employees who either have access to or process personal data have completed the awareness training offered.	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 inspected documentation that the data processor has assessed the need for a data protection officer. We have inspected documentation that the DPO has been involved in relevant tasks.	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.	*XMedicus Systems ApS' control activity*	*Test performed by Grant Thornton*	*Result of test*
C.9	The processor keeps a record of categories of processing activities for each data controller. Management has ensured that the record of categories of processing activities for each controller includes: • Name and contact information of the data processor, the data controller, representatives of the data controller and data protection officers • The categories of processing, carried out on behalf of the individual data controller. • When relevant, information about transfer to third countries or an international organisation, with documentation of adequate guarantees. • Where possible, a general description of technical and organisational security measures. 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 inspected that the categories of processing contain the following information: • the name and contact details of the processor, and the data protection officer • the categories of processing carried out on behalf of each controller • where applicable, transfers of personal data to a third country or an international organisation • where possible, a general description of the technical and organisational security measures. We have inspected that the categories of processing activities have been updated and approved by management.	No deviations noted.

Control objective D - Return and deletion of personal data

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

No.	*XMedicus Systems ApS' control activity*	*Grant Thornton's test*	*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 inspected that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller. We have inspected that the procedures are up to date.	No deviations noted.
D.2	Specific requirements have been agreed with respect to the data processor's storage periods and deletion routines.	We have inspected that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines. We have, by sample test, inspected that the latest data processing agreement contains specific requirements in regard to deletion and storing of personal data.	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 inspected that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data. We have, by sample test, inspected that the agreed deletion or return of data has taken place for terminated data processing sessions.	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.	*XMedicus Systems ApS' control activity*	*Test performed by Grant Thornton*	*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 inspected that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements. We have inspected that the procedures are up to date.	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 inspected that the data processor has a complete and updated list of processing activities stating localities, countries, or regions. We have, by sample test, inspected that documentation exists that the processing of data, including the storage of personal data, takes place only in the localities stated in the data processing agreement – or otherwise as approved by the data controller.	No 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.	*XMedicus Systems ApS' control activity*	*Test performed by Grant Thornton*	*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 inspected that formalised procedures are in place for using subprocessors, including requirements for sub-data processing agreements and instructions. We have inspected that procedures are up to date.	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 subprocessors used. We have, by sample test, inspected that documentation exists that the processing of data by the subprocessor is stated in the data processing agreements – or otherwise as approved by the data controller.	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 inspected that formalised procedures are in place for informing the data controller when changing the subprocessors used. We have inquired into whether there have been any changes to subprocessors.	We have been informed that there have been no changes in the use of subprocessors, which is why we have not been able to test the implementation of the control. 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 inspected signed sub-data processing agreements with subprocessors used, which are stated on the data processor's list. We have, by sample test, inspected that sub-data processing agreements include the same requirements and obligations as are stipulated in the data processing agreements between the data controllers and the data processor.	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.	*XMedicus Systems ApS' control activity*	*Test performed by Grant Thornton*	*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 subprocessors used. We have, by sample test, inspected that documentation exists that the processing of data by the subprocessor is stated in the data processing agreements – or otherwise as approved by the data controller.	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 inspected that formalised procedures are in place for following up on processing activities at subprocessors and compliance with the sub-data processing agreements. We have inspected documentation that each subprocessor and the current processing activity at such processor are subjected to risk assessment. We have inspected documentation that technical and organisational measures, security of processing at the subprocessors and similar matters are appropriately followed up on.	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.	*XMedicus Systems ApS' control activity*	*Grant Thornton's test*	*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 inspected that formalised procedures exist to ensure that personal data are not transferred to third countries. We have inspected that procedures are up to date.	We have been informed that personal data are not transferred to third countries, wherefore we have not been able to test the implementation of the control. 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.	*XMedicus Systems ApS' control activity*	*Test performed by Grant Thornton*	*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 inspected that 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 inspected that procedures are up to date.	No deviations noted.
H.2	The data processor has established procedures in so 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 inspected that the procedures in place for assisting the data controller include detailed procedures for: • Handing out data • Correcting data • Deleting data • Restricting the processing of personal data • Providing information about the processing of personal data to data subjects. We have inspected documentation that the systems and databases used support the performance of the relevant 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 are responded to in accordance with the data processing agreement entered into.

No.	*XMedicus Systems ApS' control activity*	*Test performed by Grant Thornton*	*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 inspected that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. We have inspected that procedures are up to date.	No deviations noted.
I.2	The data processor has established controls to identify any personal data breaches.	We have inspected that the data processor provides awareness training to the employees in identifying any personal data breaches. We have inspected documentation that network traffic is monitored and that anomalies, monitoring alarms, large file transfers, etc. are followed up on. We have inspected documentation that logging of access to personal data is continuously followed up on.	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 with an indication of whether the individual incident has resulted in a breach of personal data security. We have inquired whether there has been a breach of personal data.	We have been informed that there have been no personal data breaches, wherefore we have not been able to test the implementation of the control. No deviations noted.

Control objective I – Managing personal data breaches

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

No.	*XMedicus Systems ApS' control activity*	*Test performed by Grant Thornton*	*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: • 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.	We have inspected that the existing procedures 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 inspected documentation that the procedures available support that measures are taken to respond to the personal data breach.	No deviations noted.