

Assurance report

XMedicus Systems ApS

Independent auditor's ISAE 3000 type 2 assurance report on information security and measures pursuant to the data processing agreement with customers using XMedicus EPJ throughout the period from 1 March 2025 to 28 February 2026

October 2026

Grant Thornton | www.grantthornton.dk
Lautrupsgade 11, 2100 København Ø
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Table of Contents

Section 1:	XMedicus Systems ApS' statement	1
Section 2:	Independent auditor's ISAE 3000 assurance report with reasonable assurance on information security and measures pursuant to XMedicus Systems ApS' data processing agreements with data controllers during the period from 1 March 2025 to 28 February 2026.....	3
Section 3:	XMedicus Systems ApS' description of processing activity for the supply of XMedicus EPJ	5
Section 4:	Control objectives, controls, tests, and results hereof.....	9

Section 1: XMedicus Systems ApS' statement

The accompanying description has been prepared for data controllers, who has signed a data processing agreement with XMedicus Systems ApS, and who has a sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the EU Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "the Regulation") have been complied with.

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

Some of the control areas, stated in XMedicus Systems ApS' description in Section 3 of supply of XMedicus EPJ, can only be achieved if the complementary user entity controls with the data controllers are suitably designed and operationally effective with XMedicus Systems ApS' controls. This assurance report does not include the appropriateness of the design and operational effectiveness of these complementary user entity controls.

XMedicus Systems ApS confirms that:

- a) The accompanying description, Section 3, fairly presents how XMedicus Systems ApS has processed personal data for data controllers subject to the Regulation throughout the period from 1 March 2025 to 28 February 2026. The criteria used in making this statement were that the accompanying description:
 - (i) Presents how XMedicus Systems ApS' processes and controls were designed and implemented, including:
 - The types of services provided, including the type of personal data processed
 - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete, and restrict processing of personal data
 - The procedures used to ensure that data processing has taken place in accordance with contract, instructions, or agreement with the data controller
 - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality
 - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation
 - The procedures supporting in the event of breach of personal data security that the data controller may report this to the supervisory authority and inform the data subjects
 - The procedures ensuring appropriate technical and organisational 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 Systems ApS, have assumed would be implemented by the data controllers and which, if necessary, in order to achieve the control objectives stated in the description, are identified in the description
 - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data

- (ii) Includes relevant information about changes in the data processor's supply of XMedicus EPJ in the processing of personal data in the period from 1 March 2025 to 28 February 2026;
 - (iii) Does not omit or distort information relevant to the scope of supply 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 supply 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 operated effectively throughout the period from 1 March 2025 to 28 February 2026. If relevant controls with sub-processors were operationally effective and data controller has performed the complementary user entity controls, assumed in the design of XMedicus Systems ApS' controls throughout the period from 1 March 2025 to 28 February 2026. The criteria used in making this statement were that:
 - (i) The risks that threatened achievement of the control objectives stated in the description were identified
 - (ii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 March 2025 to 28 February 2026.
- 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, 19 October 2026
XMedicus Systems ApS

Harald Madsen
CFO

Mikkel Kruse Johnsen
CEO

Section 2: Independent auditor's ISAE 3000 assurance report with reasonable assurance on information security and measures pursuant to XMedicus Systems ApS' data processing agreements with data controllers during the period from 1 March 2025 to 28 February 2026

To: XMedicus Systems ApS and their customers

Scope

We were engaged to provide assurance about a) XMedicus Systems ApS' description, Section 3 of supply of XMedicus EPJ in accordance with the data processing agreement with data controllers throughout the period from 1 March 2025 to 28 February 2026 and about b+c) the design and operational effectiveness of controls related to the control objectives stated in the Description.

XMedicus Systems ApS uses the following sub-processors: KMD A/S and ONLINECITY.IO ApS. This statement does not include control objectives and related controls at XMedicus Systems ApS' sub-processors. 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-processor.

Some of the control objectives stated in XMedicus Systems ApS' description in Section 3 of supply of XMedicus EPJ, can only be achieved if the complementary user entity controls with the data controller 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 user entity controls.

Our opinion is based on reasonable assurance.

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; and for the design and implementation of operationally effective 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 applies International Standard on Quality Management 1, ISQM 1, requiring that we maintain 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 operational effectiveness 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 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 supply of XMedicus EPJ 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 included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved.

An assurance engagement of this type also includes evaluating the overall presentation of the Description, the 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 supply 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 how XMedicus Systems ApS' supply of XMedicus EPJ was designed and implemented throughout the period from 1 March 2025 to 28 February 2026.
- (b) the controls related to the control objectives stated in the description were suitably designed and implemented throughout the period from 1 March 2025 to 28 February 2026 in all material respects, and
- (c) the controls tested, which were the controls necessary for providing reasonable assurance that the control objectives in the description were achieved in all material respects, operated throughout the period from 1 March 2025 to 28 February 2026.

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' supply of 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.

Copenhagen, 19 October 2026

Grant Thornton

Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Martin Brogaard Nielsen
Partner, CISA, CIPP/E, CRISC

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

Purpose of the description

The purpose of this system description is to provide information to XMedicus Systems ApS' customers and their stakeholders (including auditors) regarding compliance with the data processing agreements with customers. Furthermore, the purpose is to provide information on processing security, the technical and organisational measures, and the division of responsibilities between data controllers (our customers) and XMedicus Systems ApS.

Nature of the processing

Processing of personal data on behalf of the data controller is primarily carried out by XMedicus Systems ApS performing the following:

- Storing data on dedicated servers and electronic storage devices.
- Processing personal data according to specific instructions from the data controller to assist with data extraction, necessary modifications, bug fixes, data conversion, and deletion of data.
- Facilitating the exchange of messages, referrals, discharge summaries (medical epicrisis), invoices, and similar documents between the data controller, the data subjects, authorities, and other stakeholders.
- Providing user support for the data controller's staff.
- Providing technical support.
- Ensuring that the data controller has access to data.
- Performing backups of the data controller's data.

Categories of personal data and data subjects

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

- **General personal data:** Including identification information such as name, address, age, family relations, email address, phone number, customer ID, general practitioner, payment details, insurance details, and authorisation number.
- **Special categories of personal data (sensitive):** Including health data, genetic data, and information regarding sexual relations and orientation.
- **Other confidential data:** Such as CPR numbers (civil registration numbers) and further specific health data.

The following categories of data subjects are covered:

- The data controller's patients (children and adults).
- The data controller's employees.

Instructions from the data controller

To the extent that XMedicus Systems ApS' employees receive instructions from the data controller that clearly fall within the agreed instructions (e.g., user support cf. Appendix C to the data processing agreement), the processing is carried out without further assessment or documentation.

If the instruction involves processing such as data extraction or other tasks that do not immediately appear in the data processing agreement, the individual employee assesses whether there might be doubts about its legality. To ensure the necessary competence to make this assessment, all employees undergo internal training and awareness training. The employees are further supported by internal documentation in the form of a "procedure for handling data processing agreements".

If the employee assesses that there may be doubt about the legality, XMedicus Systems ApS' DPO is requested to carry out an assessment. In these cases, both the received instruction and the assessment itself are documented.

Risk assessment

Concrete risk assessments of the processing activities are carried out, and all risk assessments are documented in the company's ISMS system. If a data controller requests assistance in carrying out a Data Protection Impact Assessment (DPIA), XMedicus Systems ApS has procedures in place to support this.

Technical and organisational security measures

XMedicus Systems ApS has implemented the following technical and organisational measures to protect personal data:

Organisational security measures:

- Drafting and maintaining policies and procedures.
- Internal training and continuous awareness training.
- In-house developed courses based on the company's core business areas.
- Continuous knowledge sharing via email and at Friday meetings.
- Preparation of an ISAE 3000 GDPR assurance report.
- Increased collaboration and purchase of services within IT security.
- Affiliation of an external DPO service from DPO Danmark.

Technical security measures:

- Use of VPN connections for secure access to servers and databases.
- Two-factor authentication and issuance of certificates for access control.
- Implementation of DNSSEC on the email server domain.
- Use of anti-phishing and anti-spoofing technologies on the email server (including DMARC, DKIM, and SPF).
- Encryption of data traffic on the email server (TLS).
- Use of centrally managed endpoint protection/antivirus on client machines.
- Continuous network monitoring and network scanning.
- Establishment of firewalls to protect server infrastructure (both front-end and back-end).
- Continuous updating of the EHR (Electronic Health Record) system.
- Network segmentation to separate and protect critical systems.
- Full disk encryption (e.g., BitLocker) on workstations.
- Regular vulnerability scanning of servers to identify irregularities.
- Automatic patch management and updating of the server infrastructure.
- Management of mounted server partitions via dedicated scripts.
- Automated data backups performed once every 24 hours.

Physical security measures:

- Burglar alarms have been established in the offices.
- The building is generally locked, and exterior doors are locked 24/7.
- Use of access cards for the facilities.
- Server cabinets are locked with a physical key.
- Physical access restriction at the hosting provider (Penta), where access requires photo identification and prior registration with the guard.
- Procedure for the technical manager to pre-order and confirm access for the individual employee on the hosting provider's internal portal.

Data Protection Officer (DPO)

Based on the nature and scope of the registered data – including the fact that the processing activity involves the regular processing of sensitive data in the form of CPR numbers – it has been assessed that XMedicus Systems ApS must have a DPO. The DPO has been appointed, is independent of the management, and is fully recognised within the organisation. Through courses, conferences, and online access to informational material, it is continuously ensured that the individual maintains the appropriate qualifications for the position.

Selection and approval

Prior to entering into agreements with sub-processors, their audit reports are obtained and reviewed. To the extent deemed necessary, supplementary information is obtained prior to entering into the agreement. Furthermore, the sub-processor agreement is reviewed to ensure it does not conflict with applicable legislation or the data processing agreements XMedicus Systems ApS has entered into with its customers. Safeguarding the data controller's rights is anchored in the sub-processor agreements with the respective supplier.

Continuous monitoring and new sub-processors

Monitoring of sub-processors is conducted annually and is primarily based on the sub-processor's audit reports. If deemed necessary, supplementary information is obtained.

In the event of changes or additions of sub-processors, the data controllers are informed of the change via email. The notification contains the necessary information about the new sub-processor and a clear text specifying that the data controller has 30 days to object to its use. XMedicus Systems ApS prepares and continuously maintains a record of all data controllers and their respective contact persons for this purpose.

Transfer of personal data

Personal data are not being transferred to unsafe third countries. Any potential data transfer to the United Kingdom takes place on the basis of the EU Commission's adequacy decision, whereby the country is approved as a safe third country.

Rights of data subjects

Section 9 of the data processing agreement states how XMedicus Systems ApS assists the data controller in fulfilling the obligation to respond to requests for exercising the rights of the data subjects, as laid down in Chapter III of the General Data Protection Regulation (GDPR).

Handling of personal data breaches

XMedicus Systems ApS has established procedures to ensure that personal data breaches are correctly identified and handled. This is ensured by:

- Continuous training of employees through awareness courses focusing on personal data security and the protection of the data subject.
- Training employees to detect potential security breaches.
- Registering possible security breaches in the company's internal incident log, which is reviewed weekly by the compliance function.
- Holding weekly meetings with all employees where relevant incidents and potential situations are reviewed.
- Using internal policies and procedures to identify and report security breaches.
- Alarm monitoring and logging on relevant systems, established by the company's CTO. In the event of deviations, a report is made to the CTO, who assesses what actions, if any, should be taken.
- A fixed procedure stating that if a significant breach is identified, the affected data controllers are informed within 24 hours of discovery.

Record of processing activities

A record of all customers (data controllers) is kept in the company's compliance software. For each data controller, the following is registered:

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

The information is updated continuously, and an annual review of the record is conducted. The general description of technical and organisational security measures can be found in the company's Information Security and Data Protection Policies, which are also continuously updated. Reference is additionally made to Section 4 of the report for a detailed description of the specific control activities.

Significant changes during the period

There have been no significant changes to the systems during the assurance period.

Complementary user entity controls at the data controller

To maintain the overall security level, the data controllers (customers) have the following obligations:

- To ensure that the user list is kept up to date. This means that the customer must immediately deactivate or delete users when an employee resigns or changes roles.
- To ensure that the processed personal data is kept up to date.
- To ensure that the instructions given are lawful in relation to the data protection legislation applicable at any given time.
- To ensure that the instruction is appropriate in relation to the data processing agreement and the main service provided.
- To ensure that the record of the data controller's users is kept up to date.
- To ensure that the necessary legal basis for processing is present.
- To comply with the duty to inform data subjects regarding the exercise of their rights.
- To verify the identity of the data subjects requesting to exercise their rights.
- The customer is responsible for having updated antivirus, firewalls, and operating systems on the PCs and devices they use to access your system.

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 functionality 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 throughout the period from 1 March 2025 to 28 February 2026.

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. The effectiveness of the controls during the audit period, is assessed by sample testing.
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 27001/2.

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	<i>New scope compared to ISO 27001/2</i>
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	<i>New scope compared to ISO 27001/2</i>
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	<i>New scope compared to ISO 27001/2</i>
D.1	6, 11, 13, 14, 32	7.4.5, 7.4.7, 7.4.4	<i>New scope compared to ISO 27001/2</i>
D.2	6, 11, 13, 14, 32	7.4.5, 7.4.7, 7.4.4	<i>New scope compared to ISO 27001/2</i>
D.3	13, 14	7.4.7, 7.4.4	<i>New scope compared to ISO 27001/2</i>
E.1	13, 14, 28, 30	8.4.2, 7.4.7, 7.4.8	<i>New scope compared to ISO 27001/2</i>
E.2	13, 14, 28, 30	8.4.2, 7.4.7, 7.4.8	<i>New scope compared to ISO 27001/2</i>
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
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	<i>New scope compared to ISO 27001/2</i>
H.2	12, 13, 14, 15, 20, 21	7.3.5, 7.3.8, 7.3.9	<i>New scope compared to ISO 27001/2</i>
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	Test 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 are in place to ensure that the processing of personal data is carried out solely in accordance with instructions. We have inspected that the procedures include requirements for at least an annual assessment of the need for updates, including in the event of changes to the data controller's instructions or changes in data processing. We have inspected that the 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 the processing of personal data is carried out solely in accordance with instructions. We have, by sample test, inspected that the processing of personal data is carried out in accordance 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 are in place to ensure control that the processing of personal data does not conflict with the General Data Protection Regulation or other legislation. We have inspected that there are procedures for notifying the data controller in cases where the processing of personal data is considered to be in violation of the law. We have inquired into whether the data processor has received instructions which, in the data processor's opinion, are infringes the General Data Protection Regulation or data protection provisions in other EU law or the national law of Member States.	We have been informed that the data processor has not received any instructions which, in the data processor's opinion, infringes the General Data Protection Regulation or data protection provisions in other EU law or the national law of Member States. 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	Test 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 that formalised procedures are in place to ensure that the agreed security measures are established. We have inspected that the procedures are up to date. We have, by sample test, inspected that the requirements for establishing security measures in the data processing agreements are in accordance with the internal procedures for this.	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 that the performed risk assessment is updated and includes the current processing of personal data. We have inspected that the data processor has implemented the security measures agreed with the data controllers.	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 that antivirus software is installed on the systems and databases used for the processing of personal data. We have, by sample test, inspected that the antivirus software has been updated during the assurance period.	We have inspected that, for one (1) out of four (4) samples, there is no evidence that antivirus control was performed from March 2025 to July 2025. No further 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 in the processing of personal data takes place only through a secured firewall. We have inspected that the firewall has been configured and 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 inspected network diagrams and other network documentation to ensure proper segmentation. We have inspected that proper segmentation has been implemented.	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	Test 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 that formalised procedures exist for restricting users' access to personal data. We have inspected that formalised procedures exist for following up to ensure that users' access to personal data is in accordance with their work-related needs. We have inspected that the agreed technical measures support the maintenance of the restriction on users' work-related access to personal data. We have inspected that work-related user access rights have been granted to employees during the assurance period.	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 that, for systems and databases used for the processing of personal data, system monitoring with alerting has been established. We have inspected documentation that follow-up on alerts has taken place during the assurance period.	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 that formalised procedures are in place to ensure that the transmission of sensitive and confidential information over the internet is protected by strong encryption based on a recognised algorithm. We have inspected that technological solutions for encryption have been available and activated throughout the entire assurance period. We have inspected that encryption is used for the transmission of sensitive and confidential personal data via the internet or by email.	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	Test performed by Grant Thornton	Result of test
B.9	Logging has been established in systems, databases, and networks. Log data are protected against manipulation, technical errors and are reviewed regularly.	We have inspected that formalised procedures exist for the configuration of logging of user activities in systems, databases, and networks used for the processing and transmission of personal data, including review and follow-up on logs. We have inspected that logging of user activities in systems, databases, and networks used for the processing and transmission of personal data is configured and activated. We have inspected that collected information about user activity in logs is protected against manipulation and deletion. We have inspected that log files contain the expected content according to the configuration, and that there is documentation for the follow-up performed and the handling of any security incidents. We have inspected that there is documentation for the follow-up performed on activities carried out by system administrators and others with special privileges.	We have inspected that the review and follow-up on logs have not followed the procedure during the audit period. As of 4 April 2025, we have inspected documentation that the procedure for reviewing and following up on logs has been updated. No further deviations noted.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	We have inspected that formalised procedures exist for the ongoing testing of technical measures, including the performance of vulnerability scans and penetration tests. We have inspected that there is documentation for the ongoing testing of the established technical measures. We have inspected that any deviations and weaknesses in the technical measures have been handled in a timely and adequate manner and have been communicated to the data controllers to the appropriate extent.	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	Test performed by Grant Thornton	Result of test
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 that formalised procedures exist for the management of changes to systems, databases, and networks, including the handling of relevant updates, patches, and security patches. We have, by sample test, inspected that changes to systems, databases, and networks have been managed in accordance with the established procedure.	We have inspected that the handling of changes to systems has not followed the procedure during the audit period. As of 4 April 2025, we have inspected documentation that the procedure for change management has been updated. No further 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 that formalised procedures exist for the granting and revocation of users' access to systems and databases used for the processing of personal data. We have inspected that documentation exists for the regular, at least annual, review and approval of granted user access rights. We have inquired whether there have been any terminated employees with access to personal data during the audit period.	We have been informed that no employees with access to personal data have been terminated during the audit period. 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 that users' access to perform processing of personal data that entails a high risk for the data subjects can only take place by using two-factor authentication.	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 formalised procedures are in place to ensure that only authorised individuals can obtain physical access to premises and data centres where personal data is stored and processed. We have inspected documentation confirming that only authorised individuals have had physical access to premises and data centres where personal data are stored and processed during the audit period.	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 that an information security policy exists, which has been reviewed and approved by management within the past year. We have inspected documentation confirming 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 documentation of management's assessment that the information security policy generally meets the requirements for security measures and processing security as set out in the concluded data processing agreements. We have, by sample test, inspected that the requirements in the data processing agreements are covered by the information security policy's requirements for security measures and processing security.	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 are in place to ensure the screening of the data processor's employees in connection with employment. We have, by sample test, inspected that the screening of employees hired during the assurance period includes obtaining of criminal records.	We have for four (4) out of four (4) samples of new employees hired during the audit period, inspected that criminal records were not reviewed at the time of employment. No further 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.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, by sample test, inspected that employees appointed during the audit period have signed a confidentiality agreement. We have, by sample test, inspected that employees appointed during the audit period have been introduced to: • Information security policy. • Procedures for processing data and other relevant information.	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 inspected procedures that ensure that the rights of terminated employees are deactivated or revoked upon termination, and that assets such as access cards, PCs, mobile phones, etc. are returned. We have inquired whether there have been any terminations during the audit period.	We have been informed that there have been no terminated employees with access to personal data during the audit period. 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 inquired whether there have been any terminations of employees with access to personal data during the audit period.	We have been informed that there have been no terminated employees with access to personal data during the audit period. 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 confirming that all employees who either have access to or process personal data have completed the offered awareness training.	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.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 confirming that the data processor has assessed the need for a data protection officer during the assurance period.	No deviations noted.
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 contains 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 • when relevant, 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 during the assurance period.	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	Test performed by Grant Thornton	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 exist for the storage and deletion of 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 the specific requirements for the data processor's retention periods and deletion routines. We have, by sample test, inspected that there is documentation confirming that personal data is stored in accordance with the agreed retention periods. We have, by sample test, inspected that there is documentation confirming that personal data have been deleted in accordance with the agreed deletion routines.	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 exist for the processing of the data controller's data upon termination of the processing of personal data. We have, by sample test, inspected that there is documentation confirming that personal data are stored in accordance with the agreed retention periods. We have, by sample test, inspected that there is documentation confirming that personal data have been deleted in accordance with the agreed deletion routines.	It has not been possible to inspect documentation confirming that the procedure for deletion of personal data was followed for one (1) out of two (2) samples. This is due to the bankruptcy of the data controller, whereby the data were delivered to the relevant authority, but the return of the data has not been documented. No further 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 there are formalised procedures in place to ensure that the storage and processing of personal data is carried out solely 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 maintains a comprehensive and up-to-date record of processing activities, specifying the locations, countries, or regions involved. We have, by sample test, inspected that there is documentation confirming that data processing, including the storage of personal data, is carried out solely at the locations specified in the data processing agreement – or otherwise 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-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-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 exist for the use of sub-processors, including requirements for sub-processor agreements and instructions. We have inspected that the procedures are up to date.	No deviations noted.
F.2	The data processor only uses sub-processors to process personal data that have been specifically or generally approved by the data controller.	We have inspected that the data processor maintains a comprehensive and up-to-date overview of the sub-processors used. We have, by sample test, inspected that there is documentation confirming that the sub-processor's data processing is reflected in the data processing agreements—or is otherwise approved by the data controller.	No deviations noted.
F.3	When changing the generally approved sub-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-processors used, this has been approved by the data controller.	We have inspected that formalised procedures exist for notifying the data controller in the event of changes in the use of sub-processors. We have inquired whether there have been any changes to sub-processors during the audit period.	We have been informed that there have been no changes in the use of sub-processors during the audit period. No deviations noted.
F.4	The data processor has subjected the sub-processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	We have, by sample test, inspected that sub-processor agreements contain the same requirements and obligations as those set out 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-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-processors.	We have inspected that the data processor maintains a comprehensive and up-to-date overview of the sub-processors used and approved. We have inspected that the overview contains, at a minimum, the required information about each individual sub-processor.	No deviations noted.
F.6	Based on an updated risk assessment of each sub-processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the sub-processor.	We have inspected that formalised procedures exist for the follow-up on processing activities at sub-processors and compliance with sub-processor agreements. We have inspected documentation confirming that a risk assessment has been performed for each sub-processor and the current processing activity at these entities. We have inspected documentation confirming that appropriate follow-up has been performed regarding technical and organisational measures, processing security at the sub-processors used, the legal basis for third-country transfers, and similar matters. We have inquired whether follow-up at sub-processors is communicated to the data controller if there are significant remarks, so that the data controller can plan any necessary audits.	We have inspected documentation confirming that reviews have been conducted with sub-processors, but for one (1) out of two (2) samples, this was finalised after the end of the audit period. No further 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	Test performed by Grant Thornton	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 are in place to ensure that personal data are only transferred to third countries or international organisations in accordance with an agreement with the data controller and based on a valid transfer mechanism. We have inspected that the procedures are up to date.	No deviations noted.
G.2	The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.	We have inspected that the data processor maintains a comprehensive and up-to-date overview of transfers of personal data to third countries or international organisations. We have inquired whether the data processor has transferred personal data to third countries or international organisations.	We have been informed that personal data are not transferred to third countries or international organisations during the audit period. No deviations noted.
G.3	As part of the transfer of personal data to third countries or international organisations, the data processor assessed and documented the existence of a valid basis of transfer.	We have inquired whether the data processor has transferred personal data to third countries or international organisations during the audit period.	We have been informed that personal data are not transferred to third countries or international organisations during the audit period. 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 exist for the data processor's assistance to the data controller in relation to the rights of data subjects. We have inspected that the procedures are up to date.	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 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 inquired whether the data processor has received any requests from the data controller in relation to the rights of data subjects.	We have been informed that the data processor has not received any requests from the data controller in relation to the rights of data subjects. 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 exist which include requirements for notifying the data controllers in the event of a personal data breach. We have inspected that the procedure is up to date.	No deviations noted.
I.2	The data processor has established controls for identification of possible personal data breaches.	We have inspected that the data processor offers awareness training to employees regarding the identification of potential personal data breaches. We have inspected documentation confirming that network traffic is monitored, and that follow-up is performed on anomalies, monitoring alerts, large file transfers, etc. We have inspected documentation confirming that timely follow-up is performed on the logging of access to personal data, including follow-up on repeated access attempts.	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-processor.	We have inspected that the data processor maintains a record of security incidents indicating whether each incident has resulted in a personal data breach. We have inquired whether there have been any personal data breaches during the audit period.	We have been informed that there have been no personal data breaches during the audit period. No deviations noted.
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 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.	No deviations noted.

PENNEO

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

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

Knud Søren Harald Madsen

XMedicus Systems ApS CVR: 38102877
CFO

Serienummer: c57fd437-0f9d-41cb-97f8-b6bde61b26dd
IP: 62.116.xxx.xxx
2026-10-19 13:38:12 UTC



Mikkel Kruse Johnsen

XMedicus Systems ApS CVR: 38102877
CEO

Serienummer: 00573261-640c-4c9f-9564-ba03ccc5e771
IP: 62.116.xxx.xxx
2026-10-19 13:40:49 UTC



Martin Brogaard Borup Nielsen

Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Partner

Serienummer: 658bcd61-1988-4367-b3eb-215cfbbb49b0
IP: 172.225.xxx.xxx
2026-10-19 13:48:00 UTC



Kristian Randløv Lydolph

Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Statsautoriseret revisor

Serienummer: 84758c07-82ce-4650-a48d-5224b246b5c4
IP: 77.241.xxx.xxx
2026-10-19 15:40:49 UTC



Dette dokument er underskrevet digitalt via **Penneo.com**. De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptografiske beviser er indlejret i denne PDF for validering i fremtiden.

Dette dokument er forseglet med et kvalificeret elektronisk segl. For mere information om Penneos kvalificerede tillidstjenester, se <https://eutl.penneo.com>.

Sådan kan du verificere, at dokumentet er originalt

Når du åbner dokumentet i Adobe Reader, kan du se, at det er certificeret af **Penneo A/S**. Dette beviser, at indholdet af dokumentet er uændret siden underskriftstidspunktet. Bevis for de individuelle underskrivers digitale underskrifter er vedhæftet dokumentet.

Du kan verificere de kryptografiske beviser vha. Penneos validator, <https://penneo.com/validator>, eller andre valideringstjenester for digitale underskrifter.