Grant Thornton

Assurance report

Creditro A/S

Independent auditor's ISAE 3000 type 2 assurance report on information security and measures pursuant to the data processing agreement with customers using Creditro Comply, Store My ID, Creditro Assess and Creditro Sign throughout the period from 1 January 2025 to 31 December 2025

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

March 2026

Table of contents

Section 1: Creditro A/S' statement

The accompanying description has been prepared for data controllers, who has signed a data processing agreement with Creditro A/S, 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.

Creditro A/S uses the following sub-processors: Microsoft, MongoDB, Mailjet, Experian and Twoday Addo. This statement does not include control objectives and related controls at Creditro A/S' 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 Creditro A/S' description in Section 3 of Creditro Comply, Store My ID, Creditro Assess and Creditro Sign, can only be achieved if the complementary user entity controls with the data controllers are suitably designed and operationally effective with Creditro A/S' controls. This assurance report does not include the appropriateness of the design and operational effectiveness of these complementary user entity controls.

Creditro A/S confirms that:

a) The accompanying description, Section 3, fairly presents how Creditro A/S has processed personal data for data controllers subject to the Regulation throughout the period from 1 January 2025 to 31 December 2025. The criteria used in making this statement were that the accompanying description:

   (i) Presents how Creditro A/S' 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 Creditro A/S, 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 Creditro Comply, Store My ID, Creditro Assess and Creditro Sign in the processing of personal data in the period from 1 January 2025 to 31 December 2025;

(iii) Does not omit or distort information relevant to the scope of Creditro Comply, Store My ID, Creditro Assess and Creditro Sign 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 Creditro Comply, Store My ID, Creditro Assess and Creditro Sign 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 January 2025 to 31 December 2025 if relevant controls with sub-processors were operationally effective and data controller has performed the complementary user entity controls, assumed in the design of Creditro A/S' controls throughout the period from 1 January 2025 to 31 December 2025.

The criteria used in making this statement were that:

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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 January 2025 to 31 December 2025.

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.

Esbjerg, 30 March 2026
Creditro A/S

Asmita Faranaz Velji
Managing Director

Section 2: Independent auditor's ISAE 3000 type 2 assurance report with reasonable assurance on information security and measures pursuant to Creditro A/S' data processing agreements with data controllers during the period from 1 January 2025 to 31 December 2025

To: Creditro A/S and their customers

Scope

We were engaged to provide assurance about Creditro A/S' description, Section 3 of Creditro Comply, Store My ID, Creditro Assess and Creditro Sign in accordance with the data processing agreement with data controllers throughout the period from 1 January 2025 to 31 December 2025 and about the design and operational effectiveness of controls related to the control objectives stated in the Description.

Creditro A/S uses the following sub-processors: Microsoft, MongoDB, Mailjet, Experian and Twoday Addo. This statement does not include control objectives and related controls at Creditro A/S' 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 Creditro A/S' description in Section 3 of Creditro Comply, Store My ID, Creditro Assess and Creditro Sign, 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 Creditro A/S. 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.

Creditro A/S' responsibilities

Creditro A/S 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 Creditro A/S' 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 Creditro Comply, Store My ID, Creditro Assess and Creditro Sign 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

Creditro A/S' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Creditro Comply, Store My ID, Creditro Assess and Creditro Sign 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 Creditro A/S' Creditro Comply, Store My ID, Creditro Assess and Creditro Sign were designed and implemented throughout the period from 1 January 2025 to 31 December 2025.

(b) the controls related to the control objectives stated in the description were suitably designed and implemented throughout the period from 1 January 2025 to 31 December 2025 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 effectively throughout the period from 1 January 2025 to 31 December 2025.

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 Creditro A/S' Creditro Comply, Store My ID, Creditro Assess and Creditro Sign 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, 30 March 2026

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Andreas Moos
Partner, CISA, CISM

Section 3: Creditro A/S' description of processing activity for the supply of Creditro Comply, Store My ID, Creditro Assess and Creditro Sign

The data controller has acquired a license for the data processor's digital solutions, where the data controller, by using the solutions, enters, uploads, imports, or otherwise adds data, including personal data, to the solutions for use.

In connection with the delivery of the digital solutions, the data processor thus processes personal data on behalf of the data controller according to applicable regulations and in accordance with the concluded data processing agreement.

Purpose of the data processor's processing of personal data on behalf of the data controller
The purpose of this description is to provide information to Creditro A/S's customers and their stakeholders (including auditors) regarding compliance with the content of the EU General Data Protection Regulation ("GDPR"). Additionally, the purpose of this description is to provide information about processing security, technical and organisational measures, and responsibilities between data controllers (our customers) and Creditro A/S.

Nature of the processing
As owner and provider of the software solutions, Creditro processes, during general operations including hosting, display, organisation, receipt, forwarding, structuring, adaptation, implementation, searching, processing, storage, recovery, deletion, restriction, maintenance, development, logging, support, troubleshooting, and other IT services, the personal data added by the data controller, as well as the personal data the data controller has enabled the data processor to add to the software.

Personal data
The types of personal data processed are:

1. Name
2. Contact information, including email address and mobile phone number
3. Relationship to company, corporation, or organisation, including role as owner, management member, position
4. Anti-money laundering reports
5. Company reports
6. Financial matters
7. Copies of identity documents
8. CPR numbers
9. Media mentions
10. Information in documents uploaded by the data controller to the data processor's service
11. Information obtained by the data processor for the data controller's use, as agreed
12. Information in documents for signature
13. Documentation for signature, including electronic ID information

Creditro processes the categories of personal data that the data controller has instructed Creditro to and informed about in the data processing agreement. However, by using the solution, the data controller may leave processing of all types of data to Creditro, given the data controller's free ability to upload or otherwise add data to the solution. If Creditro becomes aware of processing types of personal data not anticipated in the data processing agreement, Creditro will notify the data controller, but it is always the data controller's responsibility to correctly specify the types of personal data included in the use of the solution. It is emphasised that Creditro does not perform checks hereof, nor can Creditro access the personal data added by the data controller without separate consent.

Categories of data subjects covered by the data processing agreement:

1. Persons whom the data controller wishes to conduct anti-money laundering investigations on.
2. Persons related to companies, corporations, or organisations about whom the data controller wishes to obtain information
3. Persons appearing in documents uploaded by the data controller to the used solutions
4. Persons about whom the data controller wishes to obtain information
5. Persons who are to sign documents
6. Persons mentioned in documents sent for signature

Creditro only processes data about the data subjects that the data controller has instructed Creditro to and informed about in the data processing agreement. However, by using the solution, the data controller may leave processing of personal data about all categories of persons to Creditro, given the data controller's free ability to upload or otherwise add data to the solution. If Creditro becomes aware of processing categories of persons not anticipated in the data processing agreement, Creditro will notify the data controller, but it is always the data controller's responsibility to correctly specify the categories of persons relevant for the intended use of the solution. It is emphasised that Creditro does not perform checks hereof, nor can Creditro access the categories of data subjects added by the data controller without separate consent.

Instruction from the data controller

The data processor may only process data on instruction from the data controller. The data processor's processing of personal data on instruction from and on behalf of the data controller occurs by the data processor generally performing the following:
General operations, including hosting, display, organisation, receipt, forwarding, structuring, adaptation, implementation, searching, processing, storage, recovery, deletion, restriction, maintenance, development, logging, support, troubleshooting, and other IT services associated with the data processor's solution(s) and/or service(s) to the data controller according to the agreement concluded between the parties.

The data processor's processing of personal data on behalf of the data controller occurs by the data processor performing the following:

Creditro Comply

The data processor must obtain information about the persons specified by the data controller regarding their possible status as PEP or RCA. Furthermore, the data processor must obtain information about whether the person is registered on public sanctions lists. Based on the information uploaded by the data controller and information obtained from third parties, Creditro must, in accordance with the data controller's instructions, assess the risk of the person's involvement or risk of involvement in money laundering or terrorist financing. In connection with Creditro Comply, the data processor continuously monitors and updates information about persons obtained by the data processor for the data controller.

Store My ID

The data processor must send invitations via email to the persons specified by the data controller with a link to create a profile in Store My ID. The recipient of the email creates a profile in Store My ID for the data controller's documentation of compliance with the anti-money laundering law, including KYC review. The data processor stores identity documents and responses to the KYC questionnaire on behalf of the data controller.
The data processor must send invitations via email to the persons specified by the data controller with a link to Store My ID referring to profile updates in Store My ID. The interval for this is set by the data controller in Store My ID.

Creditro Assess

The data processor must obtain information about financial and credit-related matters concerning companies and persons on instruction from the data controller. The data processor must analyse the information in the score models defined and/or approved by the data controller. The data processor must, on behalf of the data controller, store obtained information and prepared analyses, and as agreed, must continuously obtain updated information regarding companies about which the data controller has obtained information.

Creditro Sign
The data processor must electronically send the documents ordered by the data controller for digital signing to the persons whom the data controller instructs the data processor to. The data processor must also register signatures and store signed documents on behalf of the data controller for the data controller's documentation.

The solutions covered by this data processing agreement are listed in the Main Agreement and any appendices to the Main Agreement.

Practical measures
Data processing is the core of the service we provide to our customers. Therefore, our customers' trust and confidence that we can deliver our service securely and confidentially is also of crucial importance to our business foundation.

We therefore take data protection and GDPR very seriously and have a continuous focus on processing our customers' data securely, including ongoing improvement of our technical and organisational security measures.

The following is a non-exhaustive list of our security measures, carried out by Creditro and/or purchased from suppliers:

- IT security policy
- Guidelines for employee security
- Asset management, including control of issuance and return of assets upon employment and termination
- Cryptography
- Supplier relations and/or supervision plan with sub-processors
- Management of personal data security breaches and incident handling
- Secure establishment of data processing agreements with sub-processors
- Ensuring that requirements imposed by law or by customers via contracts and data processing agreements are similarly imposed on sub-processors
- Control and updating of risk assessment, policies, and procedures
- Ongoing training of employees in GDPR
- Control of access based on work-related needs

Use of sub-processors
Procedures and controls are followed to ensure that only approved sub-processors are used, and that the data processor, by following up on their technical and organisational measures to protect the rights of data subjects and the processing of personal data, ensures adequate processing security.

When Creditro uses a sub-processor in connection with performing specific processing activities on behalf of the data controller, Creditro ensures, through a contract or other legal document under EU law or national law of member states, to impose on the sub-processor the same data protection obligations as those set out in the data processing agreement between Creditro and the data controller, thereby providing the necessary guarantees that the sub-processor will implement technical and organisational measures in such a way that the processing complies with the requirements of the data processing agreement and the data protection regulation. Creditro is therefore responsible for requiring that the sub-processor at least complies with Creditro's obligations under the concluded data processing agreement and the data protection regulation.

Sub-processor agreements and any subsequent amendments are available on Creditro's websites, enabling the data controller to ensure that equivalent data protection obligations as required by these provisions are imposed on the sub-processor. Provisions regarding commercial terms that do not affect the data protection content of the sub-processor agreement are not made available to the data controller.

Risk assessment
Creditro has mapped the risk to the rights of data subjects, including an assessment of these risks in relation to the precautions taken to protect these rights. The risk assessment consists of several parts, including:

- Mapping all risks associated with the processing and categorising (scoring, probability, and severity) thereof
- Assessing what are appropriate technical and organisational measures to ensure compliance with the regulation and that this can be documented

In Creditro's own risk assessments, there is no high risk for data subjects across all types of data subjects and categories of personal data.

Control measures
Creditro has established an annual cycle for systematic measurement and control of processing security. Conclusions from controls in the annual cycle are continuously evaluated and at least once a quarter by management. Required and adopted improvements in connection with this are made continuously, and notification thereof is found in newsletters to data controllers. Creditro has established a number of measures and controls to ensure compliance with the Data Protection Regulation and the concluded data processing agreements.

The established measures and controls include the following control objectives:

- Control objective A:
  - Procedures and controls are followed to ensure that instructions regarding the processing of personal data are complied with in accordance with the concluded data processing agreement.

- Control objective B:
  - Procedures and controls are followed to ensure that the data processor has implemented technical measures to ensure relevant processing security.

- Control objective C:
  - Procedures and controls are followed to ensure that the data processor has implemented organisational measures to ensure relevant processing security.

- Control objective D:
  - Procedures and controls are followed to ensure that personal data can be deleted or returned if agreed with the data controller.

- Control objective E:
  - Procedures and controls are followed to ensure that the data processor only stores personal data in accordance with the agreement with the data controller.

- Control objective F:
  - Procedures and controls are followed to ensure that only approved sub-processors are used, and that the data processor, by following up on their technical and organisational measures to protect the rights of data subjects and the processing of personal data, ensures adequate processing security.

- Control objective G:
  - Procedures and controls are followed to ensure that the data processor only transfers personal data to third countries or international organisations in accordance with the agreement with the data controller based on a valid transfer basis.

- Control objective H:
  - Procedures and controls are followed to ensure that the data processor can assist the data controller with the delivery, correction, deletion, or restriction of information about the processing of personal data to the data subject.

- Control objective I:
  - Procedures and controls are followed to ensure that any security breaches can be handled in accordance with the concluded data processing agreement.

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

Transfer of personal data
Any transfer of personal data to third countries or international organisations may only be carried out by the data processor based on documented instructions from the data controller and must always be in accordance with Chapter V of the Data Protection Regulation.

Without documented instructions from the data controller, Creditro cannot, within the framework of the data processing agreement:

1. transfer personal data to a data controller or data processor in a third country or an international organisation
2. leave processing of personal data to a sub-processor in a third country
3. process personal data in a third country

The data controller's instructions regarding the transfer of personal data to a third country, including the possible transfer basis in Chapter V of the Data Protection Regulation on which the transfer is based, are specified in Annex C, C.6 of the data processing agreement.

Rights of data subjects
Creditro assists, considering the nature of the processing, as far as possible the data controller by means of appropriate technical and organisational measures in fulfilling the data controller's obligation to respond to requests for the exercise of the data subjects' rights as established in Chapter III of the Data Protection Regulation.

This means that Creditro, as far as possible, assists the data controller in ensuring compliance with:

a) the duty to inform when collecting personal data from the data subject
b) the duty to inform if personal data are not collected from the data subject
c) the right of access
d) the right to rectification
e) the right to erasure ("the right to be forgotten")
f) the right to restriction of processing
g) the duty to notify in connection with rectification or erasure of personal data or restriction of processing
h) the right to data portability
i) the right to object
j) the right not to be subject to a decision based solely on automated processing, including profiling

Handling of personal data security breaches
Creditro notifies the data controller without undue delay after becoming aware that a personal data security breach has occurred.

Notification to the data controller is made, if possible, no later than 24 hours after Creditro becomes aware of the breach, so that the data controller can fulfil its obligation to report the breach to the competent supervisory authority, cf. Article 33 of the Data Protection Regulation.

In accordance with the concluded data processing agreement, Creditro assists the data controller in reporting the breach to the competent supervisory authority. This means that Creditro must assist in providing the following information, which according to Article 33(3) must be included in the data controller's report of the breach to the competent supervisory authority:

a) the nature of the personal data security breach, including, if possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected personal data records
b) the likely consequences of the personal data security breach
c) the measures taken or proposed by the data controller to address the personal data security breach, including, if relevant, measures to mitigate its possible adverse effects

Annex C of the data processing agreement contains further information that Creditro provides in connection with its assistance to the data controller in its obligation to report personal data security breaches to the competent supervisory authority.

Record
Creditro maintains a record of all categories of processing activities carried out on behalf of data controllers.

Creditro's management has ensured that the record of categories of processing activities for each data controller includes:

- Name and contact information of the data processor, the data controllers, any representatives of the data controller, and data protection advisors
- The categories of processing carried out on behalf of each data controller
- Where relevant, information about transfers to a third country or an international organisation and documentation of appropriate safeguards
- If possible, a general description of technical and organisational security measures

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

Complementary controls by the data controllers

In addition to the data processor's control measures, it is the data controller's responsibility to ensure the following:

- Since it is solely the data controller who, by using the solution, unilaterally enters, uploads, imports, or otherwise adds data, including personal data, to the solution, the data controller must ensure that the use of the solution only occurs according to the types of data subjects and categories of personal data agreed upon in the data processing agreement concluded between the parties.
- When requesting support, it is also the data controller's responsibility to ensure that access is only given to, or such information is shared as the resolution of the support request requires.
- The data controller must ensure that accesses and rights to the solution are correct.
- The data controller must ensure that the instruction is lawful in relation to the applicable data protection regulation at all times and ensure that the instruction is appropriate in relation to the subscription agreement for delivery of the digital solution and the data processing agreement concluded in that connection.
- When choosing the solution, the data controller is aware of the function for deleting data. The solution thus supports and presupposes that the data controller must itself perform deletion or withdrawal of data, including added personal data. The data controller may, upon request, have Creditro carry this out as further described in the concluded data processing agreement.
- The solution also supports the data controller's responsibility in requests from data subjects, which the data controller will thus be able to fulfil itself, although Creditro acknowledges its obligation to assist upon request.

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 January 2025 to 31 December 2025.

Our statement, does not apply to controls, performed at Creditro A/S' sub-processors.

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

We performed our test of controls at Creditro A/S by the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at Creditro A/S. 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 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
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.	*Creditro A/S' 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 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 inspected that a sample of 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, contravene 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, contravene the data protection regulation or data protection provisions in other EU law or the national law of the 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.	*Creditro A/S' 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 exist to ensure establishment of the safeguards agreed. We have inspected that procedures are up to date.	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 formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security. We have inspected that the risk assessment performed is up to date and comprises the current processing of personal data. We have inspected that the data processor has implemented the technical measures ensuring an appropriate level of security consistent with the risk assessment. We have inspected that the data processor has implemented the safeguards agreed with the data controller.	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, for the systems and databases used in the processing of personal data, antivirus software has been installed. We have inspected that antivirus software is up to date.	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 in the processing of personal data takes place only through a secured firewall. We have inspected that the firewall has been configured in accordance with the relevant internal policy.	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.	*Creditro A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	We have inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. We have inspected network diagrams and other network documentation to ensure appropriate segmentation.	No deviations noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	We have inspected that formalised procedures are in place for restricting users' access to personal data. We have inspected that formalised procedures are in place for following up on users' access to personal data being consistent with their work-related need. We have inspected that access is restricted to the employees' work-related need for a sample of users' access to systems and databases.	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 a written procedure has been established for the implementation of system monitoring with an alarm function. We have inspected that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. We have inspected that alarms were followed up on.	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.	*Creditro A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
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 transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognised algorithm. We have inspected that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	No deviations noted.
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 setting up logging of user activities in systems, databases or networks that are used to process and transmit personal data, including review of and follow-up on logs. We have inspected that logging of user activities in systems, databases or networks that are used to process or transmit personal data has been configured and activated. We have inspected that user activity data collected in logs are protected against manipulation or deletion. We have, by sample test, inspected that the content of a sample of log files is as expected compared to the setup and that documentation exists regarding the follow-up performed and the response to any security incidents. We have inspected that documentation exists for the follow-up performed for activities carried by system administrators and others holding special rights.	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.	*Creditro A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.	We have inspected that formalised procedures exist for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised form. We have, by sample test, inspected that personal data included in development or test databases are pseudonymised or anonymised.	No 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 regularly testing technical measures, including for performing vulnerability scans and penetration tests. We have inspected samples that documentation exists regarding regular testing of the technical measures established. We have inspected that any deviations or weaknesses in the technical measures have been responded to in a timely and satisfactory manner and communicated to the data controllers as appropriate.	No 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 that formalised procedures exist for handling changes to systems, databases, or networks, including handling of relevant updates, patches, and security patches. We have inspected extracts from technical security parameters and setups that systems, databases, or networks have been updated using agreed changes and relevant updates, patches, and security patches.	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 that formalised procedures exist for granting and removing users' access to systems and databases using to process personal data. We have inspected that documentation exists that user accesses granted are evaluated and authorised on a regular basis – and at least once a year.	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.	*Creditro A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
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 formalised procedures exist to ensure that two-factor authentication is applied in the processing of personal data that involves a high risk for the data subjects. We have inspected that users' access to processing personal data that involve 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 exist to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed. We have inspected documentation that, throughout the assurance period, only authorised persons have had physical access to premises and data centres at which personal data are stored and processed.	No 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.	*Creditro A/S' 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 that management has considered and approved within the past year. We have inspected documentation 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 safeguards and the security of processing in the data processing agreements entered into. We have, by sample test, inspected that the requirements in data processing agreements are covered by the requirements of the information security policy for safeguards and security of processing.	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 screening of the data processor's employees as part of the employment process. We have, by sample test, inspected that there is documentation that the testing of new employees includes relevant background checks.	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 employees appointed during the assurance period have signed a confidentiality agreement. We have inspected that employees appointed during the assurance period have been introduced to: • Information security policy. • Procedures for processing data and other relevant information.	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.	*Creditro A/S' 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 inspected that rights have been deactivated or terminated and that assets have been returned for employees resigned or dismissed during the assurance 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 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 provides awareness training to the employees covering general IT security and security of processing related to personal data. We have inspected documentation that all employees who have either access to or process personal data have completed the awareness training provided.	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.	*Creditro A/S' 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 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 documentation exists of personal data being stored in accordance with the agreed storage periods in data processing agreements. We have, by sample test, inspected that documentation exists that personal data are deleted in accordance with the agreed deletion routines in data processing agreements.	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 documentation exists that the agreed deletion or return of data has taken place for terminated data processing sessions during the assurance period.	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.	*Creditro A/S' 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-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.	*Creditro A/S' 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 are in place for using sub-processors, 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-processors to process personal data that have been specifically or generally approved by the data controller.	We have inspected that the data processor has a complete and updated list of sub-processors used. We have, by sample test, inspected that documentation exists that the processing of data by the sub-processor 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-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 are in place for informing the data controller when changing the sub-processors used. We have inspected documentation that the data controller was informed when changing the sub-processors used throughout 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 inspected for existence of signed sub-data processing agreements with sub-processors used, which are stated on the data processor's list. We have 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-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.	*Creditro A/S' 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 has a complete and updated list of sub-processors used and approved. We have inspected that, as a minimum, the list includes the required details about each 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 are in place for following up on processing activities at sub-processors and compliance with the sub-data processing agreements. We have inspected documentation that each sub-processor 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 sub-processors used, third countries' bases of transfer 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.	*Creditro A/S' 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 exist to ensure that personal data are only transferred to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. We have inspected that 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 has a complete and updated list 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 is not transferred to third countries or international organisations. 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 is not transferred to third countries or international organisations. 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.	*Creditro A/S' 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 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 requests from the data controller in relation to the rights of the data subjects.	We have been informed that the data processor has not received requests from the data controller in relation to the data subjects' rights. 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.	*Creditro A/S' 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 for identification of possible 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, including follow-up on repeated attempts to gain access, is followed up on, on a timely basis.	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 has a list of security incidents disclosing whether the individual incidents involved a personal data breach. We have inspected that all personal data breaches recorded at the data processor or the sub-data processors have been communicated to the data controllers concerned without undue delay after the data processor became aware of the personal data breach.	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.	*Creditro A/S' 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 procedures in place for informing the data controllers in the event of any personal data breach include detailed procedures for: • Describing the nature of the personal data breach • Describing the probable consequences of the personal data breach • Describing measures taken or proposed to be taken to respond to the personal data breach. We have inspected documentation that, when a personal data breach occurred, measures were taken to respond to such breach.	No deviations noted.

PENNEO

The signatures in this document are legally binding. The document is signed using Penneo™ secure digital signature. The identity of the signers has been recorded, and are listed below.

"By my signature I confirm all dates and content in this document."

Asmita Faranaz Velji
Creditro A/S CVR: 39181169
Underskriver 1
Serial number: 0c52d250-c0af-46f6-8a5d-414528a28591
IP: 77.173.xxx.xxx
2026-03-30 07:59:46 UTC

Mit ID

Andreas Moos
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 2
Serial number: 8ba4bf1c-2aac-4cbe-9a4b-48056ec67035
IP: 62.243.xxx.xxx
2026-03-30 08:30:25 UTC

Mit ID

Kristian Randløv Lydolph
Underskriver 3
Serial number: 7b9e0bc5-648f-4c07-87a8-debb5e403de6
IP: 62.243.xxx.xxx
2026-03-30 09:08:18 UTC

Mit ID