ABAKION A/S

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT AT 18 JANUARY 2024 ON THE DESCRIPTION OF DIGITAL BUSINESS SOLUTIONS AND RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN, RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH ACT ON SUPPLEMENTARY PROVISIONS

CONTENTS

1. INDEPENDENT AUDITOR'S REPORT

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT AT 31 DEMBER 2023 ON THE DESCRIPTION OF DIGITAL BUSINESS SOLUTIONS AND RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH ACT ON SUPPLEMENTARY PROVISIONS

To: The Management of Abakion A/S
Abakion A/S' Customers

Scope

We have been engaged to report on Abakion A/S' (the Data Processor) description in section 3 of Digital Business Solutions and the related technical and organisational measures and other controls, relating to processing and protection of personal data in accordance with the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions to the Regulation (Danish Data Protection Act), and on the design of the technical and organisational measures and other controls related to the control objectives stated in the description at 18 January 2024.

We have not performed procedures regarding the operating effectiveness of the controls stated in the description, and accordingly, we do not express an opinion on this.

The Data Processor's Responsibilities

The Data Processor is responsible for preparing the statement in section 2 and the accompanying description including the completeness, accuracy, and method of presenting the statement and the description. Furthermore, the Data Processor is responsible for providing the services covered by the description; stating the control objectives; and designing and implementing controls to achieve the stated control objectives.

Auditor's Independence and Quality Control

We have complied with the requirements of independence and other ethical requirements of the International Ethics Standards Board of Auditors' International Guidelines on the Conduct of Auditors (IESBA Code), which are based on the fundamental principles of integrity, objectivity, professional competence, and due diligence, confidentiality, and professional conduct, as well as ethical requirements applicable in Denmark.

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

Auditor's Responsibilities

Our responsibility is to express an opinion on the Data Processor's description in section 3 and on the design of the controls related to the control objectives stated in the description, based on our procedures.

We conducted our engagement in accordance with the International Standard on Assurance Engagements 3000, "Reports Other Than Audits or Reviews of Historical Financial Information". That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are appropriately designed.

An assurance engagement to report on the description and design of controls at a Data Processor involves performing procedures to obtain evidence about the disclosures in the Data Processor's description, and about the design of the 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. An assurance engagement of this type also includes evaluating the overall presentation of the description, the appropriateness of the objectives stated therein, and the suitability of the criteria specified by the Data Processor and described in section 2.

As described above, we have not performed procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, we do not express an opinion on this.

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

The Data Processor's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the use of Digital Business Solutions, that each individual Controller may consider important in their own environment. Also, because of their nature, controls at a Processor may not prevent or detect all breaches of the personal data security.

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 Data Processor's statement in section 2. In our opinion, in all material respects:

a. The description presents fairly Abakion A/S' Digital Business Solutions and the related technical and organisational measures and other controls, relating to processing and protection of personal data in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act, as designed and implemented at 18 January 2024, and

b. The technical and organisational measures and other controls, relating to the control objectives stated in the description were appropriately designed 18 January 2024

Description of Test of Controls

The specific controls tested, and the results of those tests are listed in section 4.

Intended Users and Purpose

This report is intended solely for data controllers who have used Digital Business Solutions, and who have a sufficient understanding to consider it along with other information, including information about the technical and organisational measures and other controls operated by the data controllers themselves when assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

Copenhagen, 25 January 2024

BDO Statsautoriseret Revisionsaktieselskab

Nicolai T. Visti
Partner, State Authorised Public Accountant

Mikkel Jon Larssen
Partner, Head of Risk Assurance, CISA, CRISC

2. ABAKION A/S' STATEMENT

Abakion A/S processes personal data in relation to Digital Business Solutions to our customers, who are Data Controllers according to the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions (the Danish Data Protection Act).

The description has been prepared for Data Controllers who have used Digital Business Solutions, and who have a sufficient understanding to consider the description along with other information, including information about the technical and organisational measures and other controls operated by the data controllers themselves in assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

Abakion A/S uses sub-processors. These sub-processor's relevant control objectives and related technical and organisational measures and other controls are not included in the accompanying description.

Abakion A/S confirms that the accompanying description in section 3 fairly presents Digital Business Solutions and the related technical and organisational measures and other controls at 18 January 2024. The criteria used in making this statement were that the accompanying description:

1. Presents Digital Business Solutions, and how the related technical and organisational measures and other controls were designed and implemented, including:
    - The types of services provided, including the type of personal data processed.
    - 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.
    - The controls that we, in reference to the scope of Digital Business Solutions, have assumed would be designed and implemented by the data controllers and which, if necessary, to achieve the control objectives stated in the description, are identified in the description.
    - The other aspects of the control environment, risk assessment process, information systems and communication, control activities and monitoring controls that are relevant to the processing of personal data.

2. Does not omit or distort information relevant to the scope of Digital Business Solutions and the related technical and organisational measures and other controls described while acknowledging that this description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Digital Business Solutions that the individual data controllers might consider important in their environment.

Abakion A/S confirms that the technical and organisational measures and other controls related to the control objectives stated in the accompanying description were suitable designed at 18 January 2024. The criteria we used in making this statement were that:

1. The risks threatening achievement of the described control objectives were identified.

2. The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

Abakion A/S confirms that appropriate technical and organisational measures and other controls were implemented and maintained to comply with the agreements with data controllers, good practices for the data processing of data and relevant requirements for data processors in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act.

Copenhagen, 25 January 2024

Abakion A/S

Kenneth Kryger Gran
CEO

3. ABAKION A/S' DESCRIPTION OF THE DIGITAL BUSINESS SOLUTIONS

ABAKION A/S

Abakion A/S is a Danish-owned company that develops software products and solutions based on Microsoft's business platforms (ERP, CRM, BI solutions and B2B e-Commerce) and assists customers with support on a number of online systems for both municipalities and various industries in the private market. Abakion A/S has offices in Copenhagen and Aarhus.

Abakion's ca. 160 employees are specialized in software development, support, and consulting, and are organized into a product department, four business lines, specialized units for architecture, project and customer management plus a finance and an administration department.

Most of Abakions services are based on Microsoft's cloud services. On Prem solutions are developed and supported for especially government sector costumers and some private sector customers.

WORKING WITH PERSONAL INFORMATION

Abakion delivers apps for Microsoft Online Software-as-a-service (SaaS) platforms, as well as on demand assistance and support on these solutions.

Microsoft Online platforms are developed and maintained by Microsoft. Microsoft guarantees security and procedures in relation to these platforms, and Abakion reviews these annually through the SOC2 reports provided by Microsoft.

Abakion processes personal information from the data controllers in connection with support and development assignments. In these cases, this is always work carried out on the customer's request.

Personal information treated includes personal name, e-mail address, phone number and identification.

PERSONAL DATA SECURITY MANAGEMENT

The overall responsibility for meeting the requirements in relation to data protection and protection of personal information, lies with Abakion CEO, Kenneth Kryger Gram. The responsibility for Abakion's processes lies with the teams that carry them out. The responsibility for having updated processes that are approved by the management lies with the teams' managers while the responsibility for the work being carried out according to the procedures lies with the employees who carry out the work.

The technical and organizational safety precautions and other controls for protection of personal information, is defined based on the risk assessment and are implemented to ensure confidentiality, integrity, and availability, as well as compliance with the GDPR. Safety precautions and controls are, in as many cases as possible automated and technically supported.

Management of the personal data security as well as the technical and organizational safety precautions and controls are structured in the following segments, for which there are defined controls.

ISO 27001	Control activities	GDPR article	IaaS	PaaS	SaaS	On Prem	LaaS
Risk assessment	• Risk assessment	• Art. 28(3)(c)	x	x	x		x
A.5: Information security policies	• Information Security Policy • Review of information security policy	• Art. 28(1)	x	x	x	x	
A.6: Organisation of information security	• Roles and responsibilities • Segregation of duties • Mobil device policy	• Art. 28(1) • Art. 28(3)(c)	x	x	x	x	

ISO 27001	Control activities	GDPR article	IaaS	PaaS	SaaS	On Prem	LaaS
	• Remote workplaces and remote access to systems and data						
A.7: Human resource security	• Recruitment of employees • Training and instruction of employees who process personal data • Non-disclosure and confidentiality agreements • Resignation of employees	• Art. 28(1) • Art. 28(3)(b)	x	x	x	x	
A.8: Processing activities	• Record of categories of processing activities • Storage of the record of processing activities • The Danish Data Protection Agency's access to the record of processing activities • Managing removeable media • Disposal of media	• Art. 30(2), (3) & (4)	x	x	x	x	(x)
A.9: Access management	• User registration and deregistration • Allocation of user access • Management of privileged access rights • Review of user access rights • Use of Secret Authentication Information • Procedure for secure log-on • Logical access control	• Art. 28(3)(c)	x	x	x	x	
A.10: Cryptography	• Policy for encryption • Administration of keys	• Art. 28(3)(c)	x	x	x	(x)	
A.11: Physical and environmental security	• Policy for clean desk and desktop	• Art. 28(3)(c)	x	x	x	x	
A.12: Operations security	• Maintaining system software • Antivirus program • Data backup • Logging in systems, databases, and networks, including logging of the use of personal data • Surveillance	• Art. 28(3)(c)				(x)	
A.13: Communication security	• Network security • Firewall • External communication connections	• Art. 28(3)(c)				(x)	
A.14: Acquisition, development, and maintenance of systems	• Development and maintenance of systems • Information security in development and changes • Separation of development-, test and production environment • Personal information in the development- and test environment • Support assignments	• Art. 25	x	x	x	(x)	
A.15: Supplier relationships	• Sub data processor agreements and instructions • Changes to approved sub-processors • Approved sub-processors • Overview of approved sub-processor • Supervision of sub-processors	• Art. 28(2) & (4)	X	x	x	x	
A.16: Information security incident management	• Responsibilities and procedures • Notification of breach of personal data security	• Art. 33(2)	x	x	x	x	

ISO 27001	Control activities	GDPR article	IaaS	PaaS	SaaS	On Prem	LaaS
	• Identification of breaches of personal data security • Learning from information security incidents						
A.18: Compliance	• Entering data processor agreements with data controller. • Instruction for processing of personal data • Illegal instruction from data controller • Rights of data subjects • Commitments on processing security, breaches of personal data security and impact assessments • Audit and inspection • Deletion of personal data • Return of personal information • Transfer of personal data to third countries • Testing, assessing, and evaluating the effectiveness of technical and organizational security measures	• Art. 28(3)(a), (c), (e)-(h) • Art. 29 • Art. 32(4) • Art. 28(10)	x	x	x	x	

(x) Advisory obligation.

RISK ASSESSMENT

Abakions management is responsible for launching initiatives to address the threat landscape, that Abakion at any given time faces, thus ensuring that safety precautions and controls are appropriate, and that the risk of personal data breach is reduced to an acceptable level.

The safety level is continuously assessed, to ensure that it is appropriate. This assessment considers risks in relation to personal information being accidentally or purposely deleted, lost, or changed, as well as any unauthorized transmission of, or access to, personal information being stored, transmitted, or otherwise treated.

As a base for updates of the technical and organizational security, measures, and other controls a risk assessment will be made once a year. The risk assessment will review the risks for and consequences of incidents that can be a threat to the personal data and thereby personal rights and freedom. The risk assessment accounts for the actual technical level and implementation costs.

TECNICAL AND ORGANIZATIONAL SECURITY MEASURES AND OTHER CONTROLS

The technical and organizational security measures and other controls considers all the processes and systems that treats personal information on behalf of the data controller. The control goals and activities listed in the control schemes is an integrated part of the following description.

Data controller guarantees

Abakion has introduced policies and procedures ensuring, that Abakion can provide adequate guarantees to complete appropriate technical and organizational security measures in a way, that the treatment meets the requirements in the GDPR and ensures protection of the data subjects rights.

Abakion has established an organization of personal data security, and has developed and implemented a, by the management approved information security policy, which will be continuously reviewed and updated. Abakion has procedures for recruitment and resignation of employees, as well as guidelines for education and instruction of employees, which is in touch with personal information, including conducting awareness and information campaigns.

Data process agreement

Abakion has introduced policies and procedures for data controller agreements ensuring that Abakion in relation to customer contracts, includes a data processing agreement that indicates the conditions for the treatment of personal information on behalf of the data controller.

Abakion uses a template for the data processing agreement in compliance with the services delivered, including information about the use of sub data controllers. The data controller agreements are signed and stored electronically.

Instruction for the processing of personal information

Abakion has introduced policies and procedures ensuring that Abakion will act according to the instructions given in the data processing agreement. The instruction is maintained with procedures that instruct the employees on how to process personal information, including who from the data controller that can give binding instructions to Abakion. The procedure will ensure that Abakion will inform the data controller when the instruction conflicts with the GDPR.

Sub-processors

Abakion has introduced policies and procedures ensuring that the sub-processors are imposed by the same data protection commitments that has been listed in the data processor agreement between the data controller and Abakion, and that the sub-processor can give adequate guarantees about protection of personal information. Procedures ensure that the data controller gives a prior specific or general written approval of the sub-processors, including a control of changes in already approved sub-processors.

Abakion considers the sub-processors and their guarantees before an agreement is closed to ensure that the sub-processor complies with the commitments Abakion is imposed by.

Abakion conducts an annual inspection with the sub-processors based on a risk assessment of the specific treatment of personal information, by obtaining accountant declarations of the type ISAE 3000, SOC2 or similar documentation.

Confidentiality and statutory obligation of confidentiality

Abakion has introduced policies and procedures ensuring confidentiality in the process of personal information. All Abakion's employees have committed to confidentiality by signing an employment contract which contains terms about confidentiality.

Technical and organizational security measures

Risk assessment

Abakion has completed the technical and organizational security measures based on a risk assessment regarding confidentiality, integrity, and availability. See more in separate section about this.

A.5 Information security policy

Abakion has drawn up a formal information security policy with accompanying instructions which have been incorporated in an information security policy. Policies are approved annually by the management, and manuals are approved when material changes are made.

A.6 Organisation of information security

Abakion has implemented controls to ensure a general management of the information security including a delegation of responsibilities and handling of material risks in accordance with the requirements of the company's management. Roles and responsibilities are defined considering the aim of proper segregation of duties.

Abakion is not obliged to appoint a Data Protection Officer, but a responsible contact person has been appointed for the data controllers.

Abakion staff manual sets out guidelines for use of mobile equipment outside the company. Only equipment, which complies with Abakion's security policy relating to protection against malicious code, can access the network from the outside and exclusively via VPN.

Abakion has introduced procedures ensuring that access for workspaces outside of Abakion's office and remote access to systems and data will happen through VPN-connections and gateways with two-factor authentication.

A.7 Human resource security

Abakion has implemented controls to ensure that employees are qualified and conscious of their tasks and responsibilities in relation to information security. HR are performing screening of potential employees before employment. A background check is made of all job candidates in accordance with business requirements and the function to be held by the employee.

Training and instruction of new employees who process personal data is carried out by the immediate manager. Annual training and regular awareness are being performed through post-it is on Abakion's internet.

All employees have signed a non-disclosure and confidentiality agreements in their employment agreement.

Abakion has implemented a procedure for offboarding employees including that employee is informed that the signed confidentiality agreement is still active after the leaving.

A.8 Processing activities

Abakion has introduced policies and procedures ensuring that a list of categories of control activities treated by the data controller is carried out. The list is regularly updated and controlled during the annual review of the policies and procedures. The list is stored electronically and will be available for Danish authorities – Datatilsynet upon request.

Abakion has prepared and implemented a procedure for managing removable media, including documenting whether personal data is stored on removable media, and these are encrypted when storing personal information.

Abakion has prepared and implemented a procedure for safe disposing of media where personal information is stored.

Abakion has introduced procedures ensuring that equipment given to a third party for service, repair or disposal, will be delivered without data disks and that used or discarded data media and disks is registered and destroyed in compliance with best practice regarding Abakion's employees or certified third party.

A.9 Access management

Abakion has introduced procedures ensuring that access to systems and data is protected by an authorization system. User accounts are created with a unique user identification and password, and the user identification is used when giving access to resources and systems. All allocation of rights in the systems will be based on a work-related need. At least once a year a review of the users and their work-related need for access, including actuality and correctness for the given user rights will be made. Procedures and controls support the process for creation, change and closure of users and their rights – and a review hereby.

The formation of requirements for length, complexity, continuously change, history of passwords – and closure of user accounts in case of futile attempts for access – will follow best practice for logical access security. There has been designed technical measures supporting these requirements.

Abakion employees' access to data controllers' information is logged.

Finally, two-factor authentication is implemented and is enforced on all computers.

A.10 Cryptography

Abakion has implemented controls to ensure correct and effective use of cryptography to protect confidentiality, authenticity and/or integrity of data.

Abakion has chosen to use Microsoft as a subcontractor when it comes to storing data. Microsoft has introduced procedures ensuring that databases, which contain personal information, is encrypted – and that the same applies for backups. Abakion controls Microsoft through peruse of SOC 2 reports yearly.

Abakion has introduced procedures ensuring that no personal information on personal devices without work-related need, exists. Abakions mobile computers are encrypted to ensure that access to data will only be possible for authorized users. Recovery keys and certificates are stored in a responsible manner in Microsoft Active Directory.

The algorithms and levels of encryption used for encryption of devices, servers and data will continuously be reviewed in relation to the current risk level.

A.11 Physical and environment security

Abakion has implemented controls to ensure that IT equipment is properly protected against unauthorised physical access and environmental incidents.

Abakion has introduced procedures ensuring that office rooms are secured against unauthorized access. Only people with a work-related or other legitimate needs have access to the offices. Customers, suppliers, and other visitors will be accompanied.

The physical security is administered and controlled by Microsoft in their data centres. Abakion, customer and third parties have no physical access to the data centres.

A.12 Operations security

Abakion has implemented controls to ensure that operation of servers and key systems is carried out in a structured and secure manner.

Abakion has introduced procedures ensuring that the software is continuously updated taking into account the suppliers' regulations and recommendations. Procedures for Patch Management include operating systems, critical services and software installed on servers and workstations.

Abakion has introduced procedures ensuring that devices with access to the network and applications are protected against virus and malware. This is ensured through continuous updates and adoption of anti-virus programs and other security systems in relation to the current risk level.

Abakion has introduced procedures ensuring backup of data, and recovery will only happen in the customers own environment and is performed and controlled by Microsoft.

Abakion has introduced procedures ensuring that logging is set up in compliance with legal and business requirements – based on a risk assessment of systems and the current threat level. Scope and quality of logged data is sufficient to identify and prove possible misuse of systems or data. Logged data is secured against loss and deletion.

Abakion has introduced procedures ensuring continuous surveillance of systems and introduced security measures.

Abakion has chosen to use Microsoft as a subcontractor and the customers solutions in Microsoft Online goes through security measures and penetration testing performed by Microsoft to ensure that systems are

introduced for the purpose of identification and to counter technical vulnerability in applications, services, and infrastructure, so loss of confidentiality, integrity and accessibility within systems and data will be avoided.

A.13 Communications security

Abakion has implemented controls to ensure that operation of material infrastructure components is carried out in a structured and secure manner.

Abakion has introduced procedures ensuring that networks for use and security are divided in several virtual networks (VLAN) where traffic between the individual network is controlled by a firewall. Servers with a built-in firewall uses this to make sure that access will only be given to the necessary services.

Abakion has introduced procedures ensuring that traffic between the internet and network is controlled by a firewall. Access from outside through the firewall is limited as much as possible and the access rights are given to specific segments. Workstations use firewall.

A.14 Acquisition, development, and maintenance of systems

Abakion has introduced policies and procedures for the development and implementation of the Jira-platform that ensures a controlled change process. Change Management systems for control of development- and change tasks will be used, and every task follows the same process, which is initiated with a risk assessment in compliance with the data protection through design and standard settings.

Development-, test- and product environment is separated. Each development- and change task runs through a sequence of tests. Procedures for version control, logging and backup has been introduced, so it is possible to reinstall earlier versions.

A.15 Supplier relationships

Abakion has procedures for handling and managing sub-processors, including passing instructions from the data controllers to sub-processors and supervising the sub-processors. Further, the process contains guidelines for approval of change in sub-processors and information/approval at Data controllers.

A.16 Information security incident management

Abakion has introduced policies and procedures ensuring that a breach on personal information security is registered with detailed information about the incident and that information about the breach will be given to the data controller without unnecessary delay after the breach on personal information security is discovered by Abakion. The registered information will make the data controller capable of assessing whether the breach on personal information security should be reported for the Danish authorities – Datatilsynet and if the registered persons should be informed.
Information security incidents are registered in Abakion's GDPR-system.

Abakion has introduced procedures to ensure continuous learning from information security incidents. Abakion conducts internal Semi-annual Security Incident Meetings with examination of past incidents and assessment of mitigating actions. The objective is to evaluate if processes need changing or further security measures need to be implemented as well as ensure continuous effectiveness and awareness of information security.

A.18 Compliance with customer requirements and regulatory and public authority requirements

Abakion has introduced policies and procedures ensuring that all compliance measures comply with the EU general data protection regulation and the Danish act on supplementary provision. Procedures include following issues:

- Guidelines for entering an agreement with a data controller
- Guidelines for entering data controllers' instruction
- Guidelines for reviewing instruction on regular basis

- Guidelines for notification of data controller in case of illegal instruction
- Guidelines for assistance to data controller with articles 32-36
- Guidelines for audit and inspection
- Guidelines for deletion and/or returning of personal information

Abakion has introduced policies and procedures ensuring that the transfer of personal information to the sub-processors in countries outside EU happens in compliance with EU-US Data Privacy Framework, standard contracts, or other valid basis of transfer and according to the instruction from the data controller.

4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND THE RESULT OF TESTS

Objective and scope

We conducted our engagement in accordance with ISAE 3000, Assurance Reports Other Than Audits or Reviews of Historical Financial Information.

BDO has performed procedures to obtain evidence of the information in Abakions' description of Digital Business Solutions and the design and implementation of the relating technical and organisational measures and other controls. The procedures elected depend on BDO's assessment, including the assessment of the risks that the description is not fairly presented and that the controls are not appropriately designed and implemented.

BDO's test of the design and implementation of the relating technical and organisational measures and other controls and their implementation has included the control objectives and related control activities selected by Abakion, and which are described in the check form below.

In the test form, BDO has described the tests carried out which were assessed necessary to obtain reasonable assurance that the stated control objectives were achieved, and that the related controls were appropriately designed and implemented at 18 January 2024.

Test procedures

Test of the design of the relating technical and organisational measures and other controls and their implementation was performed by inquiries, inspection, and observation.

Type	Description
Inquiry	Inquiries of relevant personnel at Abakion A/S have been performed for all significant control activities. The purpose of the inquiries was to obtain knowledge and further information about implemented policies and procedures, including how the control activities are performed, and to obtain confirmed evidence of policies, procedures, and controls.
Inspection	Documents and reports, which include information about the performance of the control, have been read for the purpose of assessing the design and monitoring of the specific controls, i.e., whether the design of the controls is such that they are expected to be effective if implemented, and whether the controls are sufficiently monitored and checked at suitable intervals. Tests have been performed of significant system structures of technical platforms, databases, and network equipment to ensure that controls have been implemented, including for example assessment of logging, back-up, patch management, authorisations and access controls, data transmission, and inspection of equipment and locations.
Observation	The use and existence of specific controls have been observed, including tests to ensure that the control has been implemented.

With respect to the services provided by Microsoft within Microsoft Azure, we have received a SOC 2 report for the period of 1 April 2022 to 31 March 2023 and associated Bridge Letter covering the period of 1 April to 30 June 2023 on technical and organisational security measures relating to Microsoft Azure.

With respect to the services provided by Continia Software within operation of Document Capture and Expense Management, we have from independent auditor received the ISAE 3402 assurance report for the sub data provider's technical and organisational security measures and other controls for the period from 1 May 2022 to 30 April 2023.

With respect to the services provided by Global Mediator within software engineering, we have from independent auditor received the ISO 27001 certificate for the sub data provider's technical and organisational security measures and other controls for the period from 3 July 2023 to 31 October 2025.

These sub-processor's relevant control objectives and related controls are not included in Abakions description of services and relevant controls related to operation of Digital Business Solution. Accordingly, we have solely assessed the report and tested the controls at Abakion that monitor the operating effectiveness of the sub-processor's controls and ensure proper supervision of the sub-processor's compliance with the data processing agreement made by the sub-processor and the data processor and compliance with the General Data Protection Regulation and the Danish Data Protection Act.

Result of test

The result of the test made of technical and organisational measures and other controls has resulted in the following exceptions noted.

An exception exists when:

- Technical and organisational measures and other controls have not been designed or implemented to fulfil a control objective, and
- Technical and organisational measures and other controls related to a control objective are not suitably designed and implemented.

Risk assessment

Control Objective

- *To ensure that the data processor carries out an annual risk assessment in relation to the consequences for the data subjects which forms basis for the technical and organisational measures.*

Control Activity	Test performed by BDO	Result of test
Risk assessment ▶ A risk assessment of Abakion's solutions is carried out based on potential risks to the availability, confidentiality, and integrity of data in relation to the data subject's rights and freedoms. ▶ The vulnerability of systems and processes is assessed based on identified threats. ▶ Risks are minimised based on the assessment of their probability, consequence, and derived implementation costs. ▶ Risk assessments are updated regularly as needed, but at least once a year.	We have made inquiries of relevant personnel at the data processor. We inspected Abakion's risk assessment and associated procedure and observed that it has been updated in 2023, as well as based on data availability, probability and derived implementation costs based on the potential risks for data subjects' rights and freedom rights. We have inspected the risk assessment and observed that it covers identified vulnerabilities of systems and processes. We have inspected the risk procedure and risk assessment and observed that risks are minimised based on the assessment of probabilities, consequences, and derived implementation costs.	No exceptions noted.

A.5: Information security policies		
Control Objective ▶ *To provide guidelines for and supporting information security and data protection in accordance with business requirements and relevant laws and regulations. GDPR art. 28, paragraph 1, art. 28, paragraph 3, point c.*		
Control Activity	**Test performed by BDO**	**Result of test**
Information security policy ▶ The data processor has developed and implemented an information security policy. ▶ The data processor has developed and implemented a policy, containing a guarantee of assistance and obligation to achieve compliance with relevant requirements, laws, and regulations.	We have made inquiries of relevant personnel at the data processor. We inspected Abakion's information security policy and observed that it has been updated in 2023. We have observed that the information security policy, include guarantee of assistance and obligation to achieve compliance with relevant requirements, laws and regulations has been made and implemented.	No exceptions noted.
Review of information security policy ▶ The data processor's information security policy is reviewed and updated at least once a year.	We have made inquiries of relevant personnel at the data processor. We inspected Abakion's information security policy and observed that it has been updated in 2023.	No exceptions noted.

A.6: Organisation of information security

Control Objective

- *To establish a management basis for initiating and managing the implementation and operation of information security and data protection in the organisation. GDPR art. 37, paragraph 1.*
- *To secure remote workplaces and the use of mobile equipment. GDPR art. 28, paragraph 3, point c.*

Control Activity	Test performed by BDO	Result of test
Roles and responsibilities ▶ The data processor has documented and established management of information security. ▶ All responsibility areas for information security and data protection have been defined and distributed. ▶ The data processor has chosen a contact point for data responsibility regarding processing of personal data.	We have made inquiries of relevant personnel at the data processor. We have observed that the information security policy, has been implemented and approved by the management. We have inspected the information security policy and observed that the responsibility for data protection has been defined and distributed. We have inspected the information security policy and observed that responsibility for information security has been assigned and distributed. We have inspected the data processor's template for data processing agreement and observed that a contact point has been chosen for the data controller with regard to the processing of personal data.	No exceptions noted.
Segregation of duties ▶ The conflicting functions and responsibilities of the data processor are separated, to the extent possible, considering the size of the company, to reduce the possibility of unauthorized or unintentional use, alteration or misuse of data.	We have made inquiries of relevant personnel at the data processor. We have inspected the technical set-up for the different roles at Abakion and observed there is a segregation of duties between the responsibilities of Abakion's employees.	No exceptions noted.
Mobile device policy ▶ The data processor has developed and implemented a policy and supportive security measures to manage the risks of personal data arising from the use of mobile devices.	We have made inquiries of relevant personnel at the data processor.	No exceptions noted.

A.6: Organisation of information security

Control Objective

- *To establish a management basis for initiating and managing the implementation and operation of information security and data protection in the organisation. GDPR art. 37, paragraph 1.*
- *To secure remote workplaces and the use of mobile equipment. GDPR art. 28, paragraph 3, point c.*

Control Activity	Test performed by BDO	Result of test
	We have inspected Abakion's mobile device policy and observed that security measures are in place.	
Remote workplaces and remote access to systems and data - All mobile devices used in a work context must have antivirus installed and updated. - Remote access to the data processor's systems and data is via an encrypted VPN connection. - Remote access must go via two-factor authentication.	We have made inquiries of relevant personnel at the data processor. By random sampling, we have inspected that antivirus is installed and updated. We have inspected Abakion's policy for organising information security and observed that remote access to the data processor's systems and data takes place via a remote gateway. We have inspected the procedure for remote access to customers' servers and observed that RDP is used to access Abakion's systems, and that RDP alongside VPN or Gateway is used to access customers' data. We have inspected that remote access goes via two-factor authentication.	No exceptions noted.

A.7: Human resource security

Control Objective

- *To ensure that employees and contracting parties understand their responsibilities and are suitable for the roles they are intended. GDPR art. 28, paragraph 1, art. 28, paragraph 3, art. 37, paragraph 1.*
- *To ensure that employees and contracting parties are aware of and meet their information security responsibilities. GDPR art. 28, paragraph 1, art. 28, paragraph 3, point c.*
- *To protect the organisation's interests as part of the change or termination of the employment relationship. GDPR art. 28, paragraph 3, point b.*

Control Activity	Test performed by BDO	Result of test
Recruitment of employees ▶ The data processor performs screening of potential employees before employment in the form of interviews and test cases. ▶ The data processor performs a background check of all job candidates in accordance with business requirements and the function to be held by the employee.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's procedure for HR and observed that candidates must be screened. By random sampling we have inspected that Abakion performs screening of potential candidates before employment We have inspected Abakion''s employment contract template. By random sampling, we have inspected that the employment contract template is used when an employee is hired.	No exceptions noted.
Training and instruction of employees who process personal data ▶ The data processor conducts instruction training of new employees in accordance with data protection and information security. ▶ Introductory course is held for new employees including on the processing of data controller's personal data. ▶ The data processor carries out ongoing training of employees in accordance with data protection and information security as well as handling thereof.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's procedure for HR and observed that employees must receive training in data protection and information security. By random sampling we have inspected that new employees receive data protection and information security training as part of their onboarding. We have inspected that Abakion annually carries out training for all employees in data protection and information security.	No exceptions noted.

A.7: Human resource security

Control Objective

- *To ensure that employees and contracting parties understand their responsibilities and are suitable for the roles they are intended. GDPR art. 28, paragraph 1, art. 28, paragraph 3, art. 37, paragraph 1.*
- *To ensure that employees and contracting parties are aware of and meet their information security responsibilities. GDPR art. 28, paragraph 1, art. 28, paragraph 3, point c.*
- *To protect the organisation's interests as part of the change or termination of the employment relationship. GDPR art. 28, paragraph 3, point b.*

Control Activity	Test performed by BDO	Result of test
Non-disclosure and confidentiality agreements ▶ All employees working with confidential data – including personal data – have signed a confidentiality agreement. ▶ External consultants are bound by a confidentiality agreement when a contract is signed.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's procedure for HR and observed that employees must sign an employment contract that contains a confidentiality agreement. We have inspected Abakion's employment contract template and observed that it contains a confidentiality agreement. By random sampling, we have inspected that employees have signed an employment contract that contains a confidentiality agreement. Upon enquiry, we have been informed that the data processor does not use external suppliers and consultants who are subject to a confidentiality agreement when entering into a contract.	No exceptions noted.
Resignation of employees ▶ The data processor has prepared and implemented a procedure for offboarding employees. ▶ Upon resignation, the employee is informed that the signed confidentiality agreement is still valid.	We have made inquiries of relevant personnel at the data processor. We have inspected the data Abakion's Procedure for HR and observed that it contains a procedure for resignation. We have inspected Abakion''s resignation template. By random sampling, we have inspected that resigning employees have returned assets and user access terminated.	No exceptions noted.

A.7: Human resource security

Control Objective

- *To ensure that employees and contracting parties understand their responsibilities and are suitable for the roles they are intended. GDPR art. 28, paragraph 1, art. 28, paragraph 3, art. 37, paragraph 1.*
- *To ensure that employees and contracting parties are aware of and meet their information security responsibilities. GDPR art. 28, paragraph 1, art. 28, paragraph 3, point c.*
- *To protect the organisation's interests as part of the change or termination of the employment relationship. GDPR art. 28, paragraph 3, point b.*

Control Activity	Test performed by BDO	Result of test
	We have inspected Abakion's Procedure for HR and observed that resigning employees are informed that the signed confidentiality agreement is still valid. By random sampling, we have inspected that employees are informed that the signed confidentiality agreement is still valid upon resignation.	

A.8: Asset management

Control Objective

- *To identify the organisation's assets and define appropriate responsibilities for its protection. GDPR art. 30, paragraph 2, art. 30, paragraph 3, art. 32, paragraph 2.*
- *To ensure adequate protection of information and personal data that is in relation to the importance of the information and personal data for the organisation. GDPR art. 30, paragraph 3, art. 30, paragraph 4.*
- *To prevent unauthorised disclosure, modification, removal or destruction of information and personal data stored on media. GDPR art. 28, paragraph 3, point c.*

Control Activity	Test performed by BDO	Result of test
Record of categories of processing activities ▶ The data processor has prepared established a record of processing activities as a data processor. ▶ The record of processing activities is continuously updated in the event of significant changes. ▶ The record of processing activities is updated at least once a year during the annual review.	We have made inquiries of relevant personnel at the data processor. We have observed that a record of processing activities as a data processor has been generated. We have inspected the annual wheel and observed that the record of processing activities is updated yearly, and we have by inquiry been informed that it also will be updated in case of significant changes.	No exceptions noted.
Storage of the record of processing activities ▶ The record of processing activities is stored electronically.	We have made inquiries of relevant personnel at the data processor. We have inspected that the record of processing activities is stored electronically.	No exceptions noted.
The Danish Data Protection Agency's access to the record of processing activities ▶ The data processor hands over the record of processing activities at the request of the Danish Data Protection Agency.	We have made inquiries of relevant personnel at the data processor. Upon enquiry, we have been informed that Abakion provides the records of processing activities at the request of the Danish Data Protection Agency. Upon enquiry, we have been informed that Abakion has not received requests from the Danish Data Protection Agency. Thus, we have not been able to test the implementation.	No exceptions noted.

A.8: Asset management

Control Objective

- *To identify the organisation's assets and define appropriate responsibilities for its protection. GDPR art. 30, paragraph 2, art. 30, paragraph 3, art. 32, paragraph 2.*
- *To ensure adequate protection of information and personal data that is in relation to the importance of the information and personal data for the organisation. GDPR art. 30, paragraph 3, art. 30, paragraph 4.*
- *To prevent unauthorised disclosure, modification, removal or destruction of information and personal data stored on media. GDPR art. 28, paragraph 3, point c.*

Control Activity	Test performed by BDO	Result of test
Managing removeable media ▶ The data processor has prepared and implemented a procedure for managing removable media, including documenting whether personal data is stored on removable media. ▶ The data processor uses encrypted moveable assets for storage of personal information.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's policy for managing removable media and observed that personal data on removable media must be handled properly. We have inspected Abakion’s encryption policy and observed that removable media for storing personal data must be encrypted. By random sampling, we have inspected that the data processor has encrypted the hard drive of computers.	No exceptions noted.
Disposal of media ▶ The data processor has prepared and implemented a procedure for disposing of media where personal information is stored in a safe manner.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion’s procedure for handling and disposal of removable media and observed that equipment must be wiped or destroyed. Upon enquiry, we have been informed that no media has been disposed of. Thus, we have not been able to test the implementation.	No exceptions noted.

A.9: Access management

Control Objective

- *To restrict access to information and personal data, including information and personal data processing facilities. GDPR art. 28, paragraph 3, point c.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services. GDPR art. 28, paragraph 3, point c.*
- *To make users responsible for securing their authentication information. GDPR art. 28, paragraph 3, point c.*
- *To prevent unauthorised access to systems and applications. GDPR art. 28, paragraph 3, point c.*

Control Activity	Test performed by BDO	Result of test
User registration and deregistration ▶ The data processor has implemented a used administration procedure that ensures that user creations and closures follow a controlled process and that all user creations are authorised.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's procedure for access management and observed that creations and closures follow the procedure. If a customer wants user-specific access, the customer himself is responsible for this, as a user is granted access from Abakion to the relevant customer's environment, after which the customer sets up the user in their environment. By random sampling, we have inspected that an employee is granted access based on a work-related need. By random sampling, we have randomly inspected that an employee's access is terminated upon resignation.	No exceptions noted.
Allocation of user access ▶ The data processor has a record of users with access to systems with personal information. ▶ User rights are allocated based on a work-related need.	We have made inquiries of relevant personnel at the data processor. We have observed that while a list of users with access to customers systems is not kept, one can from Abakion's system identify who has access to customers' systems and thereby access to systems with personal information. By random sampling, we have inspected that an employee is granted access based on a work-related need.	No exceptions noted.

A.9: Access management

Control Objective

- *To restrict access to information and personal data, including information and personal data processing facilities. GDPR art. 28, paragraph 3, point c.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services. GDPR art. 28, paragraph 3, point c.*
- *To make users responsible for securing their authentication information. GDPR art. 28, paragraph 3, point c.*
- *To prevent unauthorised access to systems and applications. GDPR art. 28, paragraph 3, point c.*

Control Activity	Test performed by BDO	Result of test
Management of privileged access rights ▶ Privileged accounts (administrative rights) to systems are granted based on a work-related need.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's procedure for access management. Upon enquiry, we been informed that all employees with access to customers' environments have "administrative rights", however, this has been deemed necessary for the employees to be able to perform their tasks.	No exceptions noted.
Review of user access rights ▶ Users and user rights are reviewed annually.	We have made inquiries of relevant personnel at the data processor. We have inspected that Abakion reviews users and user rights annually.	No exceptions noted.
Use of secret authentication information ▶ The data processor has established rules for password requirements, which must be followed by all employees as well as external consultants.	We have made inquiries of relevant personnel at the data processor. We have inspected the procedure for use of passwords and observed an excerpt of the AD password policy from which we could observe that password requirements are enforced on all employees and external consultants.	No exceptions noted.

A.9: Access management

Control Objective

- *To restrict access to information and personal data, including information and personal data processing facilities. GDPR art. 28, paragraph 3, point c.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services. GDPR art. 28, paragraph 3, point c.*
- *To make users responsible for securing their authentication information. GDPR art. 28, paragraph 3, point c.*
- *To prevent unauthorised access to systems and applications. GDPR art. 28, paragraph 3, point c.*

Control Activity	Test performed by BDO	Result of test
Procedure for secure log-on ▶ The data processor has established logical access control for systems with personal data, including two-factor authentication.	We have made inquiries of relevant personnel at the data processor. We have inspected that Abakion has established logical access control for systems with two-factor authentication.	No exceptions noted.
Logical access control ▶ A log is kept for all accesses to systems and data.	We have made inquiries of relevant personnel at the data processor. We have inspected that all access to systems and data is logged.	We have found that the retention period of the log is too short. No further exceptions noted.

A.10: Cryptography

Control Objective

- *To ensure the correct and effective use of cryptography to protect the confidentiality, authenticity and / or integrity of information and personal data. GDPR art. 28, paragraph 3, point c.*

Control Activity	Test performed by BDO	Result of test
Policy for the use of cryptography ▶ The data processor has implemented an encryption policy for encrypting personal data. The policy defines the strength and protocol of encryption. ▶ Portable media is encrypted. ▶ Encryption is used for the transmission of confidential and sensitive personal information via the internet and e-mail.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's encryption policy and observed that personal data must be encrypted. We have inspected Abakion's encryption policy and observed that portable media with personal data must be encrypted. By random sampling, we have inspected that portable media are encrypted. We have inspected Abakion''s encryption policy and observed that e-mails must be encrypted if confidential or sensitive personal data is transmitted.	No exceptions noted.
Administration of keys ▶ The Encryption keys are stored in a location other than where encrypted data is stored.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's policy for encryption and observed that keys must be stored in another location. We have inspected that encryption keys are stored in a location that is different from where encrypted data is stored.	No exceptions noted.

A.11: Physical and environmental security

Control Objective

- *To prevent unauthorised physical access to, and damage/disruption of the organisation's information and personal data, including information- and personal data processing facilities. GDPR art. 28, paragraph 3, point c.*
- *To avoid loss, damage, theft or compromise of assets and disruptions in the organization. GDPR art. 28, paragraph 3, point c.*

Control Activity	Test performed by BDO	Result of test
Policy for clean desk and desktop ▶ The Screen lock is activated after 15 minutes. ▶ Employees activate screen lock when they leave their computer.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's domain policy and observed that the screen lock is automatically activated after 15 minutes. We have inspected Abakion's employee handbook and observed that the clients must be locked when leaving the office.	No exceptions noted.

A.12: Operations security

Control Objective

- *To ensure proper and safe operation of information and data processing facilities. GDPR Art. 25, Art. 28, paragraph 3, point c.*
- *To ensure that information and personal data, including information and data processing facilities are protected against malware. GDPR Art. 28, paragraph 3, point c.*
- *To protect against data loss. GDPR Art. 28, paragraph 3, point c.*
- *To record events and provide evidence. GDPR Art. 33, paragraph 2.*
- *To ensure the integrity of operating systems. GDPR Art. 28, paragraph 3, point c.*
- *To prevent technical vulnerabilities being exploited. GDPR Art. 28, paragraph 3, point c.*
- *To minimise the impact of audit activities on operating systems. GDPR Art. 28, paragraph 1.*

Control Activity	Test performed by BDO	Result of test
Maintaining system software ▶ The data processor has implemented a process for updating system software with regards to ensuring the systems' availability and security. ▶ Operating systems software on workstations are regularly updated.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's procedure for maintaining system software and observed that system software on mobile devices, servers, SaaS platforms and on-premises is continuously updated. By random sampling, we have randomly inspected that Abakion continuously updates system software on workstations. By random sampling, we have randomly inspected that Abakion continuously updates system software on servers.	No exceptions noted.
Antivirus program ▶ Antivirus software is installed on all servers and workplace stations. ▶ Antivirus software is constantly updated and updated with the latest version.	We have made inquiries of relevant personnel at the data processor. By random sampling, we have inspected that antivirus is installed and continuously updated on the computer. By random sampling, we have inspected that antivirus is installed and continuously updated on servers.	No exceptions noted.
Data backup ▶ Systems and data are backed up daily.	We have made inquiries of relevant personnel at the data processor.	No exceptions noted.

A.12: Operations security

Control Objective

- *To ensure proper and safe operation of information and data processing facilities. GDPR Art. 25, Art. 28, paragraph 3, point c.*
- *To ensure that information and personal data, including information and data processing facilities are protected against malware. GDPR Art. 28, paragraph 3, point c.*
- *To protect against data loss. GDPR Art. 28, paragraph 3, point c.*
- *To record events and provide evidence. GDPR Art. 33, paragraph 2.*
- *To ensure the integrity of operating systems. GDPR Art. 28, paragraph 3, point c.*
- *To prevent technical vulnerabilities being exploited. GDPR Art. 28, paragraph 3, point c.*
- *To minimise the impact of audit activities on operating systems. GDPR Art. 28, paragraph 1.*

Control Activity	Test performed by BDO	Result of test
	We have inspected Abakion's procedure for backup and observed that backups are carried out daily. We have inspected that backups are carried out daily. By random sampling, we have inspected that failed backups are rectified.	
Logging in to systems, databases, and networks, including logging of the use of personal data ▶ All successful and unsuccessful attempts to access the data processor's systems and data are logged.	We have made inquiries of relevant personnel at the data processor. We have inspected that all successful and unsuccessful attempts to access the data processor's systems and data are logged.	No exceptions noted.
Surveillance ▶ The data processor has established a surveillance system of the production environment surveillance e.g., uptime, performance, and capacity. ▶ The data processor is notified regarding identified alarms and there is followed up on such.	We have made inquiries of relevant personnel at the data processor. We have inspected that Abakion has established a monitoring system. We have inspected that Abakion follows up on unidentified alarms.	No exceptions noted.

A.13: Communications security

Control Objective

- *To ensure protection of network information and personal data and supportive information and personal data processing facilities. GDPR art. 28, paragraph 3, point c.*
- *To maintain information security and data protection when transferring internally in an organisation and to an external entity. GDPR art. 28, paragraph 3, point c.*

Control Activity	Test performed by BDO	Result of test
Network security ▶ Network topology is structured according to best practise so that servers that manage the application cannot be reached directly from the internet. ▶ The data processor's network is separated so the internal server cannot communicate directly with the internet. ▶ The data processor uses well-known network technologies and mechanisms to protect the internal network.	We have made inquiries of relevant personnel at the data processor. We have observed that VPN, Gateway, and two-factor authentication are used to protect servers. We have inspected Abakions physical network and observed that Abakions network is separated so internal servers cannot communicate directly with the internet. We have observed that firewalls have been set-up on Abakion's VLAN.	No exceptions noted.
Firewall ▶ The data processor only uses services/ports which are needed. ▶ Firewalls are configurated and validated periodically an as needed to ensure that services/ports only are opened as they are needed.	We have made inquiries of relevant personnel at the data processor. We have inspected relevant documentation and observed that Abakion only uses services/ports which are needed. We have inspected that firewalls are configurated and observed that firewalls are validated periodically and as needed.	No exceptions noted.
External communication connections ▶ External connection to systems and databases, which are used to process personal data, occurs through secure firewall and VPN.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's policy for organising information security and observed that remote access to the Abakion's systems and data takes place via a remote gateway.	No exceptions noted.

A.14: System acquisition, development, and maintenance of systems

Control Objective

- *To ensure that information security and data protection is an integral part of information systems throughout the life cycle. This also includes the requirements for information systems that provide public network services. GDPR art. 25.*
- *To ensure that information security and data protection is organised and implemented within the information systems development life cycle. GDPR art. 25.*
- *To ensure the protection of data used for testing. GDPR art. 25.*

Control Activity	Test performed by BDO	Result of test
Development and maintenance of systems ▶ The data processor works based on the principles of privacy-by-design in development and maintenance assignments. ▶ Risk evaluations of systems changes are done, to ensure data protection by design.	We have made inquiries of relevant personnel at the data processor. We have inspected that Abakion works based on security-by-design principles in development and maintenance assignments.	We have established that the data processor does not carry out risk assessments of system changes, but this is expected to be incorporated in the future. No further exceptions noted.
Information security in development and changes ▶ The data processor works based on the principles of security-by-design in development and maintenance assignments. ▶ Rollback is ensured through version-controlled source codes in case of failures in the production environment. ▶ Users are generally created with lowest level of user rights. ▶ Solely the data processor's developers and project leaders with a work-related need have access to the source codes.	We have made inquiries of relevant personnel at the service provider. We have inspected that Abakion works based on security-by-design principles in development and maintenance assignments. By random sampling we have inspected that the rollback plan has been implemented in the event of errors in the production environment We have inspected that user are created with the lowest level of user rights. We have inspected that Abakions's developers have access to source code when there is a work-related need.	No exceptions noted.
Separation of development, test, and production environments ▶ Segregation between development and operations have been made. ▶ Changes in functionalities are tested before they are put into production.	We have made inquiries of relevant personnel at the data processor.	No exceptions noted.

A.14: System acquisition, development, and maintenance of systems

Control Objective

- *To ensure that information security and data protection is an integral part of information systems throughout the life cycle. This also includes the requirements for information systems that provide public network services. GDPR art. 25.*
- *To ensure that information security and data protection is organised and implemented within the information systems development life cycle. GDPR art. 25.*
- *To ensure the protection of data used for testing. GDPR art. 25.*

Control Activity	Test performed by BDO	Result of test
▶ Development and test are done in the development environment which is separated from the test environment. ▶ A version controlling system is used to register changes to the source code. ▶ Development and test environment is separated.	We have inspected that functional separation between development and operation has been introduced. The environments are divided into production, test, and development environment. We have been informed that a sandbox of the production environment has been created and that it is a perfect copy of the production environment which is why the requirements to access it is the same as for the production environment. By random sampling, we have inspected that changes are tested before they are put into production. By random sampling, we have inspected that changes are tested in development environments that are separate from production systems before they are put into operation. We have observed that branches are used as version controlling system to register source code changes.	
Personal information in the development- and test environment. ▶ Anonymised test data is used in the development and test environment.	We have made inquiries of relevant personnel at the data processor. Since a sandbox environment is used, anonymised test data is not used in development and test. This, however, is evaluated to be okay as the sandbox has the same security settings as the production environment.	No exceptions noted.
Support assignments ▶ Supporter's access and handling of personal data is solely performed based on a work-related need.	We have made inquiries of relevant personnel at the data processor.	No exceptions noted.

A.14: System acquisition, development, and maintenance of systems

Control Objective

- *To ensure that information security and data protection is an integral part of information systems throughout the life cycle. This also includes the requirements for information systems that provide public network services. GDPR art. 25.*
- *To ensure that information security and data protection is organised and implemented within the information systems development life cycle. GDPR art. 25.*
- *To ensure the protection of data used for testing. GDPR art. 25.*

Control Activity	Test performed by BDO	Result of test
	We have inspected Abakion's procedure for support tasks. By random sampling, we have randomly inspected that supporters' access and handling of personal data is based on a work-related need.	

A.15: Supplier relationships

Control Objective

- *To ensure protection of the organisation's assets and personal data that suppliers have access to. GDPR Art. 28, paragraph 2, Art. 28, paragraph 3, point d, Art. 28, paragraph 4.*
- *To maintain an agreed level of information security, data protection and delivery of services under the supplier agreements. GDPR Art. 28, paragraph 2, Art. 28, paragraph 3, point d, Art. 28, paragraph 4.*

Control Activity	Test performed by BDO	Result of test
Sub-data agreements and instruction ▶ When using sub-data processors, a data processing agreement is entered between Abakion and their sub-data processor. ▶ Instructions from the data processor is passed on to the sub-data processor. ▶ The data processing agreement with the sub-data processor is stored electronically. ▶ The data processing agreement with sub-data processors contains information on the use of sub-data processors.	We have made inquiries of relevant personnel at the data processor. We have inspected that Abakion has entered into a data processing agreement with all sub-data processors. We have inspected that instructions from Abakion is passed on to the sub-data processor. We have inspected that data processing agreements with sub-data processors are stored electronically. We have inspected that Abakion has entered into a data processing agreement with all sub-data processors. We have inspected that data processor agreements entered into with sub-processors contain information about sub-processors.	No exceptions noted.
Changes to approved sub-processors ▶ The data processor has prepared an appropriate process with the data controller for the replacement of approved sub-data processor. ▶ The data processor notifies the data controller when replacing the sub-data processor in connection with general approval of the sub-data processor. ▶ The data controller an object to the replacement of the sub-data-processor.	We have made inquiries of relevant personnel at the data processor. We have inspected the data processor's template for data processor agreement and observed that an appropriate process has been drawn up with the data controller for the replacement of approved sub-processors. By random sampling, we have inspected a concluded data processor agreement and observed that an appropriate process has been drawn up with the data controller for the replacement of approved sub-processors.	No exceptions noted.

A.15: Supplier relationships		
Control Objective ▶ *To ensure protection of the organisation's assets and personal data that suppliers have access to. GDPR Art. 28, paragraph 2, Art. 28, paragraph 3, point d, Art. 28, paragraph 4.* ▶ *To maintain an agreed level of information security, data protection and delivery of services under the supplier agreements. GDPR Art. 28, paragraph 2, Art. 28, paragraph 3, point d, Art. 28, paragraph 4.*		
Control Activity	**Test performed by BDO**	**Result of test**
	We have inspected the data processor's template for data processor agreements and observed that the data processor must notify the data controller and obtain general approval when sub-processors are replaced. By random sampling we have inspected a concluded data processing agreement and observed that the data processor must notify the data controller and obtain a general approval when replacing sub-data processors. We have inspected the data processor's template for data processor agreements and observed that the data controller has the option of objecting to the replacement of sub-processors. By random sampling, we have inspected a concluded data processor agreement and observed that the data controller has the opportunity to object to the replacement of sub-processors. Upon inquiry, we have been informed that the data processor has not replaced sub-data processors. Thus, we have not been able to test the implementation.	
Approved sub-processors ▶ The data processor has an overview of approved sub-data processors.	We have made inquiries of relevant personnel at the data processor. Upon enquiry, we have been informed and confirmed by Abakion's management that Microsoft, Continia Software, Global Mediator and Enavate are approved sub-data processors, and that the data processor therefore only uses approved sub-data processors. We have inspected Abakion's template for data processor agreement and observed that it contains the approved sub-processors.	No exceptions noted.

A.15: Supplier relationships

Control Objective

- *To ensure protection of the organisation's assets and personal data that suppliers have access to. GDPR Art. 28, paragraph 2, Art. 28, paragraph 3, point d, Art. 28, paragraph 4.*
- *To maintain an agreed level of information security, data protection and delivery of services under the supplier agreements. GDPR Art. 28, paragraph 2, Art. 28, paragraph 3, point d, Art. 28, paragraph 4.*

Control Activity	Test performed by BDO	Result of test
	By random sampling, we have inspected a concluded data processing agreement and observed that it contains approved sub-data processors.	
Overview of approved sub-processors ▶ The data processor has an overview of approved sub-data processors. An overview of approved sub-data processors contains, among other things, who is the contact person, location for processing and the type of processing and category of personal data the sub-data processor processes.	We have made inquiries of relevant personnel at the data processor. We have inspected the overview of approved sub-data-processors and observed the information about the contact person, location for processing and the type of processing and category of personal data that the sub-data processor process.	No exceptions noted.
Supervision of sub-processors ▶ The data processor performs inspections, including obtaining and reviewing the sub-data processor's auditor's statements, certification and the like. ▶ The data processor performs supervision of the sub-data processor at least once a year.	We have made inquiries of relevant personnel at the data processor. We have inspected that Abakion has carried out supervision of Microsoft by obtaining and SOC 1 and 2 as well as the Bridge Letter. We have inspected that Abakion has carried out supervision of Continia Software by obtaining and ISAE 3402. We have inspected that Abakion has carried out supervision of Global Mediator by obtaining and reviewing the ISO 27001 certificate. We have inspected that Abakion has not carried out supervision of Evanate, but that they will later carry out a supervision.	We have found that Abakion has not carried out sufficient supervision of Enavate. No further exceptions noted.

A.15: Supplier relationships

Control Objective

- *To ensure protection of the organisation's assets and personal data that suppliers have access to. GDPR Art. 28, paragraph 2, Art. 28, paragraph 3, point d, Art. 28, paragraph 4.*
- *To maintain an agreed level of information security, data protection and delivery of services under the supplier agreements. GDPR Art. 28, paragraph 2, Art. 28, paragraph 3, point d, Art. 28, paragraph 4.*

Control Activity	Test performed by BDO	Result of test
	We have inspected SOC 2 type II for the period 1 April 2022 to 31 March 2023 for Microsoft Azure. We have obtained and inspected ISAE 3402 for the period 1 May 2022 to 30 April 2023 for Continia Software. We have obtained and inspected the ISO 27001 certificate for the period 3 July 2023 to 31 October 2025 for Global Mediator.	

A.16: Information security incident management

Control Objective

- *To ensure a uniform and effective method of managing information security breaches and personal data breaches, including communication on security incidents and weaknesses. GDPR Art. 33, paragraph 2.*

Control Activity	Test performed by BDO	Result of test
Responsibilities and procedures ▶ Management responsibilities and roles have been established in connection with breaches of personal data security. ▶ The data processor has implemented a procedure for breaches of personal data security.	We have made inquiries of relevant personnel at the data processor. We have observed that a procedure for breaches of personal data security has been implemented. We have observed that management responsibilities and roles in connection with breaches of personal data security has been defined in the relevant procedure.	No exceptions noted.
Notification of breach of personal data security ▶ The data processor notifies the data controller of breaches of personal data security without undue delay. ▶ The data processor updates the data controller with all relevant and necessary information when it is available to the data processor. ▶ Communication between data processor and data controller is documented and stores.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's procedure for breaches of personal data security and observed that the data processor notifies the data controller of breaches of personal data security without undue delay. We have inspected Abakion's procedure for breaches of personal data security and observed that the data processor updates the data controller with all relevant and necessary information when it is available to the data processor. Upon enquiry, we have been informed that communication between data processor and data controller will be documented and stored. Upon enquiry, we have been informed that there have been no breaches of personal data security. Thus, we have not been able to test the implementation.	No exceptions noted.

A.16: Information security incident management

Control Objective

- *To ensure a uniform and effective method of managing information security breaches and personal data breaches, including communication on security incidents and weaknesses. GDPR Art. 33, paragraph 2.*

Control Activity	Test performed by BDO	Result of test
Registration of breaches of personal data security ▶ The data processor registers data breaches in a data breach log. ▶ The data processor has developed and implemented a procedure for experience collection after occurred data breaches.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's procedure for breaches of personal data security and observed that breaches of personal data security must be registered in the data breach log. We have inspected Abakion's data breach log and observed that no breaches of personal data security have been registered. We have inspected Abakions's procedure for breaches of personal data security and observed that a procedure for gathering experience in the event of breaches of personal data security is in place. Upon enquiry, we have been informed that there have been no breaches of personal data security. Thus, we have not been able to test the implementation.	No exceptions noted.

A.18: Compliance

Control Objective

- *To prevent violations of statutory, regulatory, or contractual requirements in relation to information security and other security requirements. GDPR Art. 25, Art. 28, paragraph 2, Art. 28, paragraph 3, point a, Art. 28, paragraph 3, point e, Art. 28, paragraph 3, point g, Art. 28, paragraph 3, point h, Art. 28, paragraph 3, point f, Art. 28, paragraph 10, Art. 29, Art. 32, paragraph 4, Art. 33, paragraph 2.*
- *To ensure that information security and data protection is implemented and run-in accordance with the organisation's policies and procedures. GDPR Art. 28, paragraph 1.*

Control Activity	Test performed by BDO	Result of test
Entering a data processor agreement with the data controller ▶ The data processor has procedures for entering into a written data processing agreements which is in accordance with the services provides by the data processor. ▶ The data processor uses its data processor agreement template when entering into data processor agreements. ▶ Data processor agreements contain information on the use of sub-data processors.	We have made inquiries of relevant personnel at the data processor. We have inspected that Abakion has a procedure for entering into written data processing agreements. We have inspected that Abakion has a template for data processor agreements. By random sampling, we have inspected that Abakion has used their template for data processing agreements when entering into the agreement. We have inspected that data processing agreements are signed and stored electronically. We have inspected Abakion's template for data processor agreements and observed that it contains information about the use of sub-processors. By random sampling we inspected a concluded data processor agreement and observed that it contains information about the use of sub-processors.	No exceptions noted.
Instruction for processing of personal data ▶ Data processing agreement containing an instruction from the data controller. ▶ The data processor obtains instructions for the processing of personal data from the data controller in connection with the conclusion of a data processor agreement.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's template for data processing agreement and observed that it contains instructions from the data controller.	No exceptions noted.

A.18: Compliance

Control Objective

- *To prevent violations of statutory, regulatory, or contractual requirements in relation to information security and other security requirements. GDPR Art. 25, Art. 28, paragraph 2, Art. 28, paragraph 3, point a, Art. 28, paragraph 3, point e, Art. 28, paragraph 3, point g, Art. 28, paragraph 3, point h, Art. 28, paragraph 3, point f, Art. 28, paragraph 10, Art. 29, Art. 32, paragraph 4, Art. 33, paragraph 2.*
- *To ensure that information security and data protection is implemented and run-in accordance with the organisation's policies and procedures. GDPR Art. 28, paragraph 1.*

Control Activity	Test performed by BDO	Result of test
	By random sampling, we have inspected a concluded data processing agreement and observed that it contains instructions from the data controller.	
Compliance with instructions for processing personal data ▶ The data processor only processes data in accordance with instructions from the data controller. ▶ The data processor has created and implemented formal procedures for processing personal data to ensure that data is only processed according to instructions from data controllers. ▶ The data processor reviews and updates its procedure at least yearly. ▶ The data processor performs self-controls to ensure that that data is only processed according to instructions from data controllers.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's procedure and observed that only processing of personal data is carried out, which appears from instructions from the data controller. We have inspected Abakion's template for data processing agreement and observed that processing of personal data takes place according to instructions from the data controller. By random sampling, we have inspected a concluded data processing agreement and observed that the processing of personal data takes place according to instructions from the data controller. We have inspected Abakions's procedure and observed that it is updated annually and in 2023. We have inspected Abakion's procedure for compliance with instructions and observed that the data processor has carried out self-control.	No exceptions noted.
Notification of the data controller in case of illegal instruction ▶ The data processor has developed a procedure for notifying the data controller, in cases where the	We have made inquiries of relevant personnel at the data processor.	No exceptions noted.

A.18: Compliance

Control Objective

- *To prevent violations of statutory, regulatory, or contractual requirements in relation to information security and other security requirements. GDPR Art. 25, Art. 28, paragraph 2, Art. 28, paragraph 3, point a, Art. 28, paragraph 3, point e, Art. 28, paragraph 3, point g, Art. 28, paragraph 3, point h, Art. 28, paragraph 3, point f, Art. 28, paragraph 10, Art. 29, Art. 32, paragraph 4, Art. 33, paragraph 2.*
- *To ensure that information security and data protection is implemented and run-in accordance with the organisation's policies and procedures. GDPR Art. 28, paragraph 1.*

Control Activity	Test performed by BDO	Result of test
data controller's instructions are contrary to the data protection legislation. ▶ The data controller shall immediately notify the data controller in cases where the data controller's instructions are in breach of data protection law.	We have inspected Abakion's procedure for notifying the data controller and observed that Abakion must notify the data controller in cases where the data controller's instructions conflict with data protection legislation. We have inspected Abakion's template for data processing agreement and observed that Abakion immediately informs the data controller in cases where the data controller's instructions are contrary to the data protection legislation. By random sampling, we inspected a concluded data processing agreement and observed that Abakion immediately informs the data controller in cases where the data controller's instructions are contrary to the data protection legislation. Upon enquiry, we have been informed that the data processor has not received instructions which are contrary to the data protection legislation. Thus, we have not been able to test the implementation.	
Rights of data subjects ▶ The data processor has developed a procedure for assistance to data controllers in fulfilling the data subjects' rights.	We have made inquiries of relevant personnel at the data processor. We have inspected that Abakion has a procedure for assistance to data controllers in fulfilling the data subjects' rights. Upon enquiry, we have been informed that Abakion has not received requests regarding the data subjects' rights. Thus, we have not been able to test the implementation.	No exceptions noted.

A.18: Compliance

Control Objective

- *To prevent violations of statutory, regulatory, or contractual requirements in relation to information security and other security requirements. GDPR Art. 25, Art. 28, paragraph 2, Art. 28, paragraph 3, point a, Art. 28, paragraph 3, point e, Art. 28, paragraph 3, point g, Art. 28, paragraph 3, point h, Art. 28, paragraph 3, point f, Art. 28, paragraph 10, Art. 29, Art. 32, paragraph 4, Art. 33, paragraph 2.*
- *To ensure that information security and data protection is implemented and run-in accordance with the organisation's policies and procedures. GDPR Art. 28, paragraph 1.*

Control Activity	Test performed by BDO	Result of test
Commitments on processing security, breaches of personal data security and impacts assessments ▶ Procedures have been established for the assistance of data controllers in compliance with articles 32-36.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's template for data processing agreement and observed that Abakion assists the data controller in compliance with articles 32-36. By random sampling, we have inspected concluded data processor agreements and observed that Abakion assists the data controller in compliance with articles. Upon enquiry, we have been informed that Abakion has not received requests from the data controller regarding assistance in compliance with articles 32-36. Thus, we have not been able to test the implementation.	No exceptions noted.
Audit and inspection ▶ The data processor is required to prepare an independent audit declaration on the technical and organisational security measures, aimed at the processing and protection of personal data. ▶ The data processor assists the data controller in physical supervision by making resources available. ▶ The data processor shall make the necessary information available to the data controller and the supervisory authority upon request in connection with the audit and inspection of the data processor.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's template for data processor agreements and observed that Abakion is required to prepare and independent audit declaration. By random sampling, we have inspected a concluded data processor agreement and observed that Abakion is required to to prepare an independent audit declaration. We have inspected Abakion's template for data processing agreements and observed that Abakion assists the data controller during physical inspections.	No exceptions noted.

A.18: Compliance

Control Objective

- *To prevent violations of statutory, regulatory, or contractual requirements in relation to information security and other security requirements. GDPR Art. 25, Art. 28, paragraph 2, Art. 28, paragraph 3, point a, Art. 28, paragraph 3, point e, Art. 28, paragraph 3, point g, Art. 28, paragraph 3, point h, Art. 28, paragraph 3, point f, Art. 28, paragraph 10, Art. 29, Art. 32, paragraph 4, Art. 33, paragraph 2.*
- *To ensure that information security and data protection is implemented and run-in accordance with the organisation's policies and procedures. GDPR Art. 28, paragraph 1.*

Control Activity	Test performed by BDO	Result of test
	By random sampling, we have inspected that Abakion assists the data controller during physical inspections. Upon enquiry, we have been informed that Abakion has not received requests from the data controller regarding physical inspections. Thus, we have therefore not been able to test the implementation. We have inspected the Abakion's template for data processing agreements and observed that the data processor assists the supervisory authority with physical inspection. By random sampling, we have inspected that Abakion assists the supervisory authority with physical inspections. Upon enquiry, we have been informed that the data processor has not received requests from the supervisory authority regarding physical inspections. Thus, we have not been able to test the implementation.	
Deletion of personal data ▶ The data processor deletes the data controller's personal data according to the instructions, upon termination of the main agreement.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's procedure for deletion of personal data. Upon enquiry, we have been informed that there have been no terminated data processing agreements where the data controller's personal data had to be deleted. Thus, we have not been able to test the implementation.	No exceptions noted.

A.18: Compliance

Control Objective

- *To prevent violations of statutory, regulatory, or contractual requirements in relation to information security and other security requirements. GDPR Art. 25, Art. 28, paragraph 2, Art. 28, paragraph 3, point a, Art. 28, paragraph 3, point e, Art. 28, paragraph 3, point g, Art. 28, paragraph 3, point h, Art. 28, paragraph 3, point f, Art. 28, paragraph 10, Art. 29, Art. 32, paragraph 4, Art. 33, paragraph 2.*
- *To ensure that information security and data protection is implemented and run-in accordance with the organisation's policies and procedures. GDPR Art. 28, paragraph 1.*

Control Activity	Test performed by BDO	Result of test
Return of personal information ▶ The data processor returns the data controller's personal information according to instructions, upon termination of the main agreement. ▶ The data controller and data processor have agreed in which format, transfer and media data is to be returned when requested by the data controller.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's procedure for return of personal data. Upon enquiry, we have been informed that there have been no terminated data processing agreements where the data controller's personal data had to be returned. Thus, we have not been able to test the implementation.	No exceptions noted.
Transfer of personal data to third countries ▶ Written procedures exist for the transfer of personal data to third countries or international organisations in accordance with the agreement with the data controller based on a valid transfer basis.	We have made inquiries of relevant personnel at the data processor. We have inspected Abakion's template for data processing agreement and observed that third-country transfers can only take place on instructions from the data controller. Upon enquiry, we have been informed that Abakion has not received any instructions regarding transfers of personal data to third countries recently. We have therefore not been able to test implementation. We have carried out an inspection of the data processing agreement with Abakion and Microsoft and observed that the transfer tool is standard contractual clauses. We have inspected that Microsoft's privacy policy contains reference to the Data Privacy Framework and that the processed types of personal data are accepted,	We have found that Abakion has entered into a collaboration with Enavate in relation to development. We have established that a number of security measures have been implemented to secure a transfer basis. We have inspected these and observed that these are not assessed as fully sufficient to comply with the Danish Data Protection Authority's guidance and GDPR for the transfer of personal data to third countries, as the following conditions are not assessed as sufficient: • A lack of transfer tool for transfer in the form of standard contractual clauses under Article 46 GDPR. • A transfer impact assessment to examine applicable legislation and practice in the third country to examine whether supplementary measures are needed has not been conducted. A valid transfer tool is therefore not provided for Enavate in cases where data controllers give instructions to allow third-country transfers. No further exceptions noted.

A.18: Compliance

Control Objective

- *To prevent violations of statutory, regulatory, or contractual requirements in relation to information security and other security requirements. GDPR Art. 25, Art. 28, paragraph 2, Art. 28, paragraph 3, point a, Art. 28, paragraph 3, point e, Art. 28, paragraph 3, point g, Art. 28, paragraph 3, point h, Art. 28, paragraph 3, point f, Art. 28, paragraph 10, Art. 29, Art. 32, paragraph 4, Art. 33, paragraph 2.*
- *To ensure that information security and data protection is implemented and run-in accordance with the organisation's policies and procedures. GDPR Art. 28, paragraph 1.*

Control Activity	Test performed by BDO	Result of test
	Upon enquiry, we have been informed that the data processor has not received support recently. Upon inquiry, we have been informed that the current data center for hosting Abakion at Microsoft is in Europe. We have inspected that Microsoft is certified under the Data Privacy Framework. Upon enquiry, we have been informed that the data processor has not received support from Microsoft recently. Upon enquiry, we have been informed that no third-country transfers have taken place to Evanate to Abakion's knowledge.	
Testing, assessing, and evaluating the effectiveness of technical and organisational security measures. - The data processor tests, assesses, and evaluates the effectiveness of the technical and organisational security measures that are appropriate in relation to the data that is handled on behalf of the data controller.	We have made inquiries of relevant personnel at the data processor. We have by inquiry been informed that relevant documentation does not exist since relevant procedures are newly made.	No exceptions noted.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

HAVNEHOLMEN 29
1561 KØBENHAVN V

CVR NO. 20 22 26 70

PENNEO

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

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

Kenneth Kryger Gram
CEO
På vegne af: Abakion A/S
Serienummer: c0f9b36d-f1b6-4a2f-894c-bd9ee1642d69
IP: 109.56.xxx.xxx
2024-01-27 13:52:31 UTC

Nicolai Tobias Visti Pedersen
Partner, State Authorised Public Accountant
På vegne af: BDO Statsautoriseret Revisionsaktiesels…
Serienummer: 096fe1fc-de80-4d55-8c69-fc2fb761227d
IP: 77.243.xxx.xxx
2024-01-28 09:31:49 UTC

Mikkel Jon Larssen
BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670
Partner, Head of Risk Assurance, CISA, CRISC
På vegne af: BDO Statsautoriseret Revisionsaktiesels…
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 62.66.xxx.xxx
2024-01-28 15:12:57 UTC