

Twoday

Independent auditor's ISAE 3000 assurance report on information security and measures during the period from 1 April 2025 to 31 March 2026 pursuant to the data processing agreement with customers using SaaS solutions and consultancy services

September 2026

Contents

1. Management's assertion.....	3
2. Independent auditor's assurance report.....	5
3. Description of processing.....	7
4. Control objectives, control activity, tests and test results	12



1. Management's assertion

Twoday Danmark A/S and Twoday Business Apps ERP A/S (hereinafter mentioned as "Twoday") processes personal data on behalf of customers in accordance with the data processing agreement.

The accompanying description has been prepared for customers who have used SaaS solutions and consultancy services and who have a sufficient understanding to consider the description along with other information, including information about controls operated by the data controller itself in assessing whether the requirements of the EU regulation on the "Protection of natural persons with regard to the processing of personal data and on the free movement of such data" and "Lov om supplerende bestemmelse til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (subsequently "the data protection rules") have been complied with.

Twoday Danmark A/S and twoday Business Apps ERP A/S are collectively referred to as 'Twoday' solely for purposes of this report. Each company remains responsible for the services and controls.

The respective Managements of Twoday Danmark A/S and twoday Business Apps ERP A/S assert that :

- a) The accompanying description in section 3 fairly presents SaaS solutions and consultancy services that have processed personal data for data controllers subject to the data protection rules during the period from 1 April 2025 to 31 March 2026. The criteria used in making this statement were that the accompanying description:
 - (i) Presents how SaaS solutions and consultancy services were designed and implemented, including:
 - The types of services provided, including the type of personal data processed
 - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete and restrict processing of personal data
 - The procedures used to ensure that data processing has taken place in accordance with contract, instructions or agreement with the data controller
 - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality
 - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation
 - The procedures supporting, in the event of breach of personal data security, that the data controller may report this to the supervisory authority and inform the data subjects
 - The procedures ensuring appropriate technical and organisational security measures in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
 - Controls that we, in reference to the scope of the SaaS solutions and consultancy services, have assumed would be implemented by the data controller and which, if necessary, in order to achieve the control objectives stated in the description, are identified in the description
 - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data.
 - (ii) Includes relevant details of changes to the controls in relation to the SaaS solutions and consultancy services during the period from 1 April 2025 to 31 March 2026
 - (iii) Does not omit or distort information relevant to the scope of the SaaS solutions and consultancy services being described for the processing of personal data, while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the SaaS solutions and consultancy services that each individual data controller may consider important in its own particular circumstances.

- b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively during the period from 1 April 2025 to 31 March 2026. The criteria used in making this statement were that:
 - (i) The risks that threatened achievement of the control objectives stated in the description were identified
 - (ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.
 - (iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, during the period from 1 April 2025 to 31 March 2026.
- c) Appropriate technical and organisational measures were established to comply with the agreements with the data controllers, sound data processing practices and relevant requirements for data processors in accordance with the data protection rules.

Copenhagen, 7 September 2026
Twoday Danmark A/S

Elias Inderberg
 Country Managing Director

Copenhagen, 7 September 2026
Business Apps ERP A/S

Carsten Andersen
 Business Unit Director

2. Independent auditor's assurance report

Independent auditor's ISAE 3000 assurance report on information security and measures during the period from 1 April 2025 to 31 March 2026 pursuant to the data processing agreement with customers

To: Twoday Danmark A/S and Twoday Business Apps ERP A/S (Twoday) and customers

Scope

We have been engaged to report on Twoday Danmark A/S and Twoday Business Apps ERP A/S (hereinafter mentioned as "Twoday")'s description in section 3 of its SaaS solutions and consultancy services in accordance with the data processing agreement with customers during the period from 1 April 2025 to 31 March 2026 (the description) and on the suitability of the design and operating effectiveness of controls related to the control objectives stated in the description.

Twoday use the following subservice organisations in the service delivery to customers:

- team.blue Denmark A/S
- Retarus GmbH
- Compaya A/S
- ITM8 A/S
- Microsoft Danmark ApS
- RelateIT DMCC

In addition Twoday uses the follow subservice organisations for hosting internal systems:

- Sentia Denmark A/S

This report uses the carve-out method, and the description in section 3 includes only the control objectives and related controls of Twoday and excludes the control objectives and related controls at subservice organisations.

The description indicates that certain control objectives specified in the description can be achieved only if the complementary controls at customers contemplated in the design of Twoday's controls are suitably designed and operating effectively. This report does not comprise the suitability of the design or operating effectiveness of such complementary controls at customers.

We express reasonable assurance in our conclusion.

Twoday's responsibilities

Twoday is responsible for: preparing the description and accompanying assertion in section 1, including the completeness, accuracy and method of presentation of the description and assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; identifying the criteria and designing, implementing and effectively operating controls to achieve the stated control objectives.

Auditor's independence and quality control

We have complied with the independence and other ethical requirements in the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct, as well as ethical requirements applicable in Denmark.

Our firm applies International Standard on Quality Management 1, 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 fairness of Twoday's description and on the suitability of the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures.

We conducted our engagement in accordance with ISAE 3000 (revised), “Assurance engagements other than audits or reviews of historical financial information”, and additional requirements applicable in Denmark to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description of a data processor’s system and on the suitability of the design and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the description and the design and operating effectiveness of controls. The procedures selected depend on the data processor’s auditor’s judgement, including the assessment of risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified by the data processor and described in section 1.

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

Limitations

Twoday’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 service delivery that the individual data controller may consider important in its own particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect all personal data breaches. Also, the projection to future periods of any evaluation of the fairness of the presentation of the description, or opinions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria including the control objectives described in Twoday’s assertion in section 1:

- a) The description fairly presents SaaS solutions and consultancy services as designed and implemented during the period from 1 April 2025 to 31 March 2026
- b) The controls related to the control objectives stated in the description were suitably designed and implemented during the period from 1 April 2025 to 31 March 2026, in all material respects, and
- c) The controls tested, which were the controls necessary for providing reasonable assurance that the control objectives in the description were achieved in all material respects, operated effectively throughout the period 1 April 2025 to 31 March 2026

Description of test of controls

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

Intended users and purpose

The report and the description of tests of controls in Section 4 are intended only for data controllers who have used Twoday’s service delivery who have a sufficient understanding to consider it along with other information, including information about controls operated by the data controllers themselves.

Copenhagen, 7 September 2026

RSM Denmark

Statsautoriseret Revisionspartnerselskab
CVR-nr. 25 49 21 45

Martin Enderberg Lassen
State-Authorised Public Accountant
Mne40044

Andreas Moos
Head of IT Risk Assurance

3. Description of processing

Twoday and our performance

We are an international and leading provider of business-critical IT-solutions in the Nordics. An IT-company, which provides software development, data- and analytics solutions, consulting service and bespoke solutions to both private and public sectors.

Across Norway, Sweden, Finland, Lithuania, and Denmark we are more than 2.700 highly skilled colleagues across several entities, who work together every day to create value through technology and data.

In Twoday Denmark A/S and Twoday Business Apps ERP A/S we help more than 8.000 customers in creating IT-solutions that makes a difference both locally, and in the larger global perspective. We know that most companies and organisations have digital transformation on the agenda. With our experience, knowledge, and approach we can help making solutions that bring a better tomorrow.

In short, we, Twoday, work today, every day, to make a better tomorrow – thru use of technology. We do this with great dedication, heart and adaptability as basis for achieving great things – with each other, our customers and society.

In the Danish company Twoday Danmark A/S we deliver bespoke software, consulting services and products to the public sector and private companies.

We deliver both products including software as a service (SaaS), and bespoke software to the public sector and large regulated private companies. For customers needing more than standard solutions we provide tailor-made solutions.

Our mission is to expand our position as the preferred partner of software solutions to enable the continuous development of the Digital Society and eGovernment in the Nordic countries. Our Governments in the Nordics have supported the Digital Society since the early 2000s. They firmly believe that digitalisation is a cornerstone in up keeping our welfare society and meet the challenges of the growing elderly population and competition from the developing countries in the future. We must simply become more efficient, and digitisation of the public sector is one important answer.

Twoday Business Apps ERP A/S – the company and services

Twoday Business Apps ERP A/S is a Microsoft Dynamics 365 Business Central/NAV partner that delivers ERP consulting services to companies with both national and international development needs. Twoday Business Apps ERP A/S also delivers solutions for customers' IT infrastructure.

The core services are:

- Consulting services and development on Microsoft Business Central/NAV & LS Central
- Sale of ISV solutions
- Digitalisation and automation of business processes

To deliver the above services and carry out IT work or support, the employees working on a given customer have access to that customer's platform.

Making the Nordics digital

We constantly work on making the Nordics digital, helping both public and private companies design, develop, modernise, and maintain software. We deliver both custom-made and commercial solutions. Together with our customers, we deliver increased productivity and growth in the Nordics for the benefit of us all. In close collaboration with the customer, we develop end-to-end business solutions and self-service solutions that help customers improve productivity through digitalisation, automation, and integration of business processes. Additionally, we provide services for maintaining, supporting, and enhancing the solutions as part of the entire lifecycle, thereby keeping the solutions updated and effective over time.

Cooperation with our customers

We work according to agile principles and in very close cooperation with our customers. Part of our DNA is to strive for customer value. We do this through professional skills using state of the art methods and tools as well as insights to challenges in the market. As a result, our solutions make an important impact in society and value for our customers' businesses.

With technically advanced expertise and knowledge of our clients, we are analysing, designing, developing, and testing new innovative software solutions to enhance competitiveness. Through implementation and integrations, we can capture, organize, store, analyse, and visualize substantial amounts of information. We also reduce bureaucracy through improved online collaboration and self-service solutions.

Our software solutions help large organisations to automate and manage straight-through processing enabling enterprises to become more efficient and profitable.

High degree of rules and regulations

Twoday is managing some of the largest ICT contracts in the public sector with values exceeding 100 MDKK each. Many of the contracts are long-term contracts (4-6 years) and include mission critical solutions with high degree of rules and regulation. Consequently, we have established long-term relations with our customers, and we invest in building value creating domain knowledge to ensure continuous satisfied customers. Some of our customers have a track record of more than 25 years.

We are constantly improving our compliance and governance setup as our business expands into other regulated sectors, and regulatory and compliance requirements change to keep up with development in technology and political landscape.

Solutions and services

Solutions and services from Twoday:

- Cloud platforms
- Cloud security and identity
- Endpoint management
- Modern workplace
- Bespoke solutions and services
- Systems development and project delivery
- Application lifecycle management
- Business intelligence
- Big data
- Machine learning
- Predictive analytics
- Business process management & straight-through processing
- Electronic signature
- Signing as a service
- E-government solutions
- Self-service solutions
- E-commerce solutions
- Content management solutions
- Mobile solutions

Compliance

Both services and products are delivered according to mutual, written, agreement between the customer and Twoday Danmark A/S. Agreements are by default based on Twoday Danmark A/S' template, tailored for our services. In cases where the agreements are based on the customer's template, including public tenders and agreements under the SKI' frame agreements, Twoday ensures that services are fit for purpose of the agreement.

Where Twoday Danmark A/S process personal data, we have entered into a data processing agreement (DPA) which outlines the basis and boundaries for the processing of personal data. DPA are by default based on Twoday Danmark A/S' standard template but can also upon mutual agreement be based on other templates. For SaaS boundaries for data processing is typically outlined in the terms of service.

Nature of processing

The purpose of the data processor's processing of personal identifiable information (PII) is based on the client's needs and instructions as stated in the Data Processing Agreement (DPA) with each client. The nature of the processing and the data differs from client to client. Twoday Danmark A/S does not store data of any EU citizen in own-hosted systems - all infrastructure related to processing of EU PII is presently located with external hosting partner.

Twoday Business Apps ERP A/S delivers services related primarily to advice and assistance to the customer, comprising setup, migration, testing, development and similar activities. Typical activities are:

- Testing of software or hardware solutions developed for the customer
- Analysis and troubleshooting in the customer's IT systems
- Migration of data between the customer's IT systems

In performing its services at customers, Twoday Business Apps ERP A/S comes into contact with customers' personal data. Personal data is always processed on the customer's own platform, and Twoday Business Apps ERP A/S' processing can therefore only take place there – Twoday Business Apps ERP A/S does not process personal data in its own systems and databases and does not transfer personal data from the customer's platform in connection with its services. It is therefore the customer's responsibility to establish appropriate security measures for the processing of personal data, such as backup, encryption and logging.

Personal information

Twoday Danmark A/S has stored in systems:

- Personal information (Name, address, email, phone etcetera)
- Classified information (CPR, income)

Categories of data subjects that are used in a DPA

- Pension takers
- Digital signers
- Pension brokers
- People in fishery (employees, ship owners, fishermen)

Practical deployments

Management in Twoday has approved all procedures, controls, internal tools, and instructions to sub data processors.

Organisationally all employees have been informed about personal identifiable data and information security, including security incident procedures - what to do in case of an incident. This happens through an e-learning course and a meeting where security awareness is presented.

Access to Twoday Danmark A/S requires access card and code, except the main entrance inside working hours where there is a staffed reception.

Risk management

As a part of each project that manages PII, the project management together with the customer does a risk analysis with regards to data risk and data subject rights according to the general Risk Management Process. Furthermore, Twoday Danmark A/S performs every year an analysis and documents all the data where Twoday Danmark A/S is data processor.

Control measures

Processing – instructions

We always do what the DPA says. We act on behalf of the data owner, who gives the instructions on what and how to process the data.

Procedure control

There is a yearly review of all procedures based on incidents, risk assessments etc. It is carried out by the data protection manager and the security officer.

Procedure for access control

Access to individual projects is given based on the respective team leads authorisation. Team lead initially presents a list of employees that need access to resources and support grants the access. Subsequent access can only be given if team lead approves. Access is also revoked on team lead request and all access (except support) is revoked upon termination of project.

The access is reviewed on a half-year basis.

Procedure for development

Most of Twoday Danmark A/S' projects are performed at client site where Twoday has little influence on how the development should be performed. For in-house development, the data protection manager visits each project yearly (and always at least once if the project lasts less than a year) and inspects if data subjects rights are managed within the project – i.e., can the project support the data subjects' rights (Can they delete data, find data on request etcetera). Projects with significant risk is visited more frequent.

Procedure for data subject's requests

The privacy mailbox is processed on daily basis by Twoday data protection council for any request, including registered data subjects, for further processing.

Procedure for security incidents

Security (and privacy) incidents are managed through incident management/SOC. They are available outside normal business hours, and they are contacted in case of breach. From there they follow a strict procedure to contain, collect information and remedy the situation.

Employees

It is stated in each employee contract that the employee is obligated to hold each client's data private.

As Twoday Business Apps ERP A/S' processing of customers' personal data takes place only on the customers' own platforms, no processing of personal data takes place in Twoday Business Apps ERP A/S' own systems and databases, and Twoday Business Apps ERP A/S does not transfer personal data from customers' platforms in connection with its services. Twoday Business Apps ERP A/S has implemented control measures that ensure its processing of customers' personal data is based on identified risks, covering the following areas:

- Data processing agreements and instructions (control objective A)
- Technical security measures (control objective B)
- Organisational measures (control objective C)
- Use of sub-processors (control objective F)
- Transfer to third countries (control objective G)
- Handling of security breaches (control objective I)
- E-mails are encrypted centrally by Twoday Business Apps ERP A/S, and all e-mails are TLS-encrypted in transit.

Sub-processors

For Twoday Denmark customer data for EU citizens are all hosted with external Danish hosting providers. Each year the reports (ISAE 3402, ISAE 3000) is evaluated by the projects using a hosting provider.

Sub processors are assessed annually, which includes checks for changes in processing activities as well as verification against EU and UN sanction lists.

Twoday Business Apps ERP A/S uses the sub-processor RelateIT DMCC, which is registered in the United Arab Emirates (Dubai). RelateIT DMCC is used in cases where assistance is needed with development and setup, to the same extent as Twoday Business Apps ERP A/S itself. A sub-processing agreement has been entered into with RelateIT DMCC, ensuring that RelateIT DMCC is subject to the same policies and procedures as Twoday Business Apps ERP A/S, and RelateIT DMCC's employees follow Twoday Business Apps ERP A/S' procedures, controls and policies. Twoday Business Apps ERP A/S does not transfer personal data to third countries without a specific agreement with the data controller, and customers may request Twoday Business Apps ERP A/S' transfer impact assessments for the United Arab Emirates.

Significant changes in the period

Twoday has since the separation from Visma in 2022 been working on a coherent company strategy, whereby streamlining business operation across all countries. This has meant establishing unified business units across all countries as well as centralising business enablement functions like IT, HR, Finance, Marketing and Communications.

A part of the coherent company journey has led to legal merger of the former Twoday entities Twoday Data & AI (former Kapacity), Twoday CPS (former CT Global), Twoday Minds (former IT Minds) and Twoday DX (former Co3) into Twoday Danmark A/S – forming Twoday Danmark A/S as of February 2025. The remaining entities are Twoday BA-CX (former TwoMany) and Twoday Business Apps ERP A/S (former Relate IT).

In September 2025 Twoday entered into agreement with Sentia Denmark A/S as provider for hosting internal systems.

Complementary user entity controls

For all our projects, where data is stored outside Twoday Danmark A/S' control – e.g., public projects where data is stored with Statens IT – this is almost all of our public projects, the agreement to store data is between the customer and Statens IT. Thus, it is Statens IT that is responsible for maintaining the security and privacy for all data stored. It is also Statens IT that controls the access to data – gives access, audits and revokes access again. Twoday Danmark A/S follows the procedures given to gain access and follows the DPA with the customer – Twoday Danmark A/S is still responsible for how its employees act within the systems hosted at Statens IT when access has been granted.

For a number of projects, Twoday Danmark A/S works together with a third party for the customer. The contract with the third party is with the customer, but Twoday Danmark A/S will exchange data with the third party. How the third party fulfils the requirements for security and privacy is agreed between the customer and the third party and it is also the customer that audits that these requirements are fulfilled.

As Twoday Business Apps ERP A/S works within customers' own environments, a number of controls under the data processing agreement remain the responsibility of the data controller to perform, including that the data controller:

- Ensures that personal data is kept up to date
- Ensures that the data processing agreement is lawful under applicable data protection regulation
- Ensures that the data processing agreement is representative of the scope of the delivery
- Has prepared a risk assessment of the processing of personal data, including a data protection impact assessment where relevant
- Assesses the risks relating to the transfer of data to third countries in connection with Twoday Business Apps ERP A/S' use of its sub-processor in Dubai, and, in that connection, establishes appropriate tech-

nical and organisational safeguards in the customer's own environments – for example appropriate logging and monitoring, alerts for suspicious activity (such as data extraction), and appropriate access restrictions, including the use of two-factor authentication

- Has established appropriate controls to secure access and rights management for its own employees and users
- Has established relevant, appropriate security measures relating to the processing of personal data, including monitoring, network segmentation and antivirus installation
- Provides assistance to data subjects, including assistance carried out via the customer's own tools

4. Control objectives, control activity, tests and test results

Purpose and scope

We conducted our engagement in accordance with ISAE 3000 (revised), “Assurance engagements other than audits or reviews of historical financial information”, and additional requirements applicable in Denmark.

Our testing of the design, implementation and operating effectiveness of the controls has included the control objectives and related control activities selected by Management and listed below.

Our testing included the control activities deemed necessary to obtain reasonable assurance that the stated control objectives were achieved.

This statement is issued according to the carve-out method and therefore does not include controls at subservice organisations.

Tests performed

The test actions performed when determining the operating effectiveness of controls are described below:

Test procedure		Description of the test procedure
Inquiries		Inquiry of appropriate personnel. Inquiries included how the controls are performed.
Observation		We observed the execution of the control.
Inspection		Reading of documents and reports containing specifications regarding the execution of the control. This includes reading and consideration of reports and other documentation in order to assess whether specific controls are designed so they may be expected to become effective if implemented. Furthermore, it is assessed whether controls are being monitored and checked sufficiently and at appropriate intervals.
Reperformance of the control		Repetition of the relevant control. We repeated the execution of the control to verify whether the control functions as assumed.

Overview of control objectives, control activity, tests and test results

Control objective A - Instructions regarding processing of personal data			
Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with in accordance with the data processing agreement entered into			
Nr.	Twoday control activity	Tests performed by RSM	Result of test
A.1	Written procedures are in place which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures are in place to ensure that personal data are only processed according to instructions. Inspected that the procedures include a requirement to assess at least once a year the need for updates, including in case of changes in the data controller's instructions or changes in the data processing. Inspected that procedures are up to date.	No exceptions noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	Inspected that Management ensures that personal data are only processed according to instructions. Inspected, by sample test, that personal data processing operation that the processing is conducted consistently with instructions.	No exceptions noted.
A.3	The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions.	Inspected that formalised procedures are in place, ensuring verification that personal data are not processed against the Data Protection Regulation or other legislation. Inspected that procedures are in place for informing the data controller of cases where the processing of personal data is considered to be against legislation.	No exceptions noted. We have noted that the data processor has not received instructions that infringe the Regulation or other European Union or member state data protection provisions.

Control objective B - Technical measures

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

Nr.	Twoday control activity	Tests performed by RSM	Result of test
B.1	Written procedures are in place which include a requirement that security measures agreed are established for the processing of personal data in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures are in place to ensure establishment of the security measures agreed. Inspected that procedures are up to date. Inspected, by sample test, that the security measures agreed have been established.	No exceptions noted.
B.2	The data processor has performed a risk assessment and, based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the security measures agreed with the data controller.	Inspected that formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security. Inspected that the risk assessment performed is up to date and comprises the current processing of personal data. Inspected that the data processor has implemented the technical measures ensuring an appropriate level of security consistent with the risk assessment. Inspected that the data processor has implemented the security measures agreed with the data controller.	No exceptions noted.
B.3	For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.	Inspected that antivirus software has been installed for the systems and databases used in the processing of personal data. Inspected that antivirus software is up to date.	No exceptions noted.
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	Inspected that external access to systems and databases used in the processing of personal data takes place only through a secured firewall. Inspected that the firewall has been configured in accordance with the relevant internal policy.	No exceptions noted.

Control objective B - Technical measures

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

Nr.	Twoday control activity	Tests performed by RSM	Result of test
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	Inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. Inspected network diagrams and other network documentation to ensure appropriate segmentation.	No exceptions noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	Inspected that formalised procedures are in place for restricting users' access to personal data. Inspected that formalised procedures are in place for following up on users' access to personal data being consistent with their work-related need. Inspected that the technical measures agreed support retaining the restriction in users' work-related access to personal data. Inspected, by sample test, that user's access to systems is restricted to the employees' work-related need.	No exceptions noted.
B.7	System monitoring with an alarm feature has been established for the systems and databases used in the processing of personal data.	Inspected that system monitoring with an alarm feature has been established for systems and databases used in the processing of personal data.	No exceptions noted.
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	Inspected that formalised procedures are in place to ensure that transmissions of sensitive and confidential personal data through the internet are protected by strong encryption based on a recognised algorithm. Inspected that technological encryption solutions are available and active. Inspected that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	No exceptions noted.

Control objective B - Technical measures

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

Nr.	Twoday control activity	Tests performed by RSM	Result of test
B.9	Logging has been established in systems, databases, and networks. Log data are protected against manipulation and technical errors and are reviewed regularly.	Inspected that formalised procedures are in place for setting up logging of user activities in systems, databases or networks that are used to process and transmit personal data, including review of and follow-up on logs. Inspected that logging of user activities in systems, databases or networks that are used to process or transmit personal data has been configured and activated. Inspected that user activity data collected in logs are protected against manipulation or deletion. Inspected, by sample test, that the content of log files is as expected compared to the set-up and that documentation confirms the follow-up performed and the response to any security incidents. Inspected, by sample test, that documentation confirms the follow-up performed on activities carried out by system administrators and others holding special rights.	No exceptions noted.
B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.	Inspected that formalised procedures are in place for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised form. Inspected, by sample test, that personal data included therein are pseudonymised or anonymised.	No exceptions noted.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	Inspected that formalised procedures are in place for regularly testing technical measures, including for performing vulnerability scans and penetration tests. Inspected that regular testing of the technical measures established is documented.	No exceptions noted.

Control objective B - Technical measures

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

Nr.	Twoday control activity	Tests performed by RSM	Result of test
B.12	Changes to systems, databases or networks are made consistently with established procedures that ensure maintenance using relevant updates and patches, including security patches.	Inspected that formalised procedures are in place for handling changes to systems, databases or networks, including handling of relevant updates, patches and security patches. Inspected extracts from technical security parameters and set-ups that systems, databases or networks have been updated using agreed changes and relevant updates, patches and security patches.	No exceptions noted.
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	Inspected that formalised procedures are in place for granting and removing users' access to systems and databases used for processing personal data. Inspected, by sample test, that user accesses granted have been authorised and that a work-related need exists. Inspected, by sample test, that access to systems and databases was deactivated or removed in a timely manner. Inspected that documentation states that user accesses granted are evaluated and authorised on a regular basis – and at least once a year.	No exceptions noted.
B.14	Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication.	Inspected that formalised procedures are in place to ensure that two-factor authentication is applied in the processing of personal data that involves a high risk for the data subjects. Inspected that users' access to processing personal data that involve a high risk for the data subjects may only take place by using two-factor authentication.	No exceptions noted.

Control objective B - Technical measures			
Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing			
Nr.	Twoday control activity	Tests performed by RSM	Result of test
B.15	Physical access security measures have been established so as to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed.	Inspected that formalised procedures are in place to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed. Inspected documentation that only authorised persons have physical access to premises and data centres at which personal data are stored and processed.	No exceptions noted.



Control objective C - Organisational measures

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

Nr.	Twoday control activity	Tests performed by RSM	Result of test
C.1	Management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The information security policy is based on the risk assessment performed. Assessments are made on a regular basis – and at least once a year – as to whether the information security policy should be updated.	Inspected that an information security policy exists that Management has considered and approved within the past year. Inspected documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No exceptions noted.
C.2	Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.	Inspected documentation of Management's assessment that the information security policy generally meets the requirements for security measures and the security of processing in the data processing agreements entered into. Inspected, by sample test, that requirements in data processing agreements are covered by the requirements of the information security policy for security measures and security of processing.	No exceptions noted.
C.3	The employees of the data processor are screened as part of the employment process.	Inspected that formalised procedures are in place to ensure screening of the data processor's employees as part of the employment process. Inspected, by sample test, that employees are screened as part of the employment process.	No exceptions noted.
C.4	Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.	Inspected, by sample test, that newly appointed employees have signed a confidentiality agreement. Inspected, by sample test, that newly appointed employees have been introduced to: • The information security policy • Procedures for processing data and other relevant information.	No exceptions noted.

Control objective C - Organisational measures

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

Nr.	Twoday control activity	Tests performed by RSM	Result of test
C.5	For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned.	Inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal and that assets such as access cards, computers, mobile phones, etc. are returned. Inspected, by sample test, that resigned or dismissed employees access rights have been deactivated or terminated and that assets have been returned.	No exceptions noted.
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	Inspected that formalised procedures are in place to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality. Inspected, by sample test, that resigned or dismissed employees confirm the continued validity of the confidentiality agreement and the general duty of confidentiality.	No exceptions noted.
C.7	Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data.	Inspected that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data. Inspected documentation stating that all employees who have either access to or process personal data have completed the awareness training provided.	No exceptions noted.

Control objective D - Return and deletion of personal data

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

Nr.	Twoday control activity	Tests performed by RSM	Result of test
D.1	Written procedures are in place which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller. Inspected that procedures are up to date.	No exceptions noted.
D.2	Specific requirements have been agreed with respect to the data processor's storage periods and deletion routines.	Inspected that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines. Inspected, by sample test, that personal data are stored in accordance with the agreed storage periods. Inspected, by sample test, that personal data are deleted in accordance with the agreed deletion routines.	No exceptions noted.
D.3	Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been: - Returned to the data controller and/or - Deleted if this is not in conflict with other legislation.	Inspected that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data. Inquired whether data processing agreements have been terminated within the audit period.	No exceptions noted. We have noted that no data processing agreement has been terminated in the period.

Control objective E - Storage of personal data

Procedures and controls are complied with to ensure that the data processor will only store personal data in accordance with the agreement with the data controller.

Nr.	Twoday control activity	Tests performed by RSM	Result of test
E.1	Written procedures are in place which include a requirement that personal data must only be stored in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures are in place for only storing and processing personal data in accordance with the data processing agreements. Inspected that procedures are up to date.	No exceptions noted.
E.2	Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.	Inspected that the data processor has a complete and updated list of processing activities stating localities, countries or regions. Inspected, by sample test, that the processing of data, including the storage of personal data, takes place only in the localities stated in the data processing agreement.	No exceptions noted.

Control objective F - Use of sub-processors

Procedures and controls are complied with to ensure that only approved sub-processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing

Nr.	Twoday control activity	Tests performed by RSM	Result of test
F.1	Written procedures are in place which include requirements for the data processor when using sub-processors, including requirements for sub-processing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures are in place for using sub-processors, including requirements for sub-processing agreements and instructions. Inspected that procedures are up to date.	No exceptions noted.
F.2	The data processor only uses sub-processors to process personal data that have been specifically or generally approved by the data controller.	Inspected that the data processor has a complete and updated list of sub-processors used. Inspected, by sample test, that the processing of data by the sub-processor follows from the data processing agreement.	No exceptions noted.
F.3	When changing the generally approved sub-processors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the data processor. When changing the specially approved sub-processors used, this has been approved by the data controller.	Inspected that formalised procedures are in place for informing the data controller when changing the sub-processors used. Inquired whether there have been changes to sub-data processors during the audit period.	No exceptions noted. We have noted that there have been no changes in sub-processors during the audit period.
F.4	The data processor has subjected the sub-processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	Inspected that sub-processors used are stated on the data processor's list. Inspected, by sample test, that requirements and obligations in sub-processing agreements includes the same requirements and obligations as are stipulated in the data processing agreement between the data controller and the data processor.	No exceptions noted.

Control objective F - Use of sub-processors

Procedures and controls are complied with to ensure that only approved sub-processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing

Nr.	Twoday control activity	Tests performed by RSM	Result of test
F.5	The data processor has a list of approved sub-processors disclosing: • Name • Company registration no. • Address • Description of the processing.	Inspected that the data processor has a complete and updated list of sub-processors used and approved. Inspected that, as a minimum, the list includes the required details about each sub-processor.	No exceptions noted.
F.6	Based on an updated risk assessment of each sub-processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the sub-processor.	Inspected that formalised procedures are in place for following up on processing activities at sub-processors and compliance with the sub-processing agreements. Inspected documentation that each sub-processor and the current processing activity at such processor are subjected to risk assessment. Inspected, by sample test, that technical and organisational measures, security of processing at the sub-processors used, third countries' bases of transfer and similar matters are appropriately followed up on.	No exceptions noted.

Control objective G - Transfer of personal data to third countries

Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.

Nr.	Twoday control activity	Tests performed by RSM	Result of test
G.1	Written procedures are in place which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures are in place to ensure that personal data are only transferred to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Inspected that procedures are up to date.	No exceptions noted.
G.2	The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.	Inspected that the data processor has a complete and updated list of transfers of personal data to third countries or international organisations. Inspected, by sample test, that transfers of personal data were arranged with the data controller in the data processing agreement or subsequently approved.	No exceptions noted.
G.3	As part of the transfer of personal data to third countries or international organisations, the data processor assessed and documented the existence of a valid basis of transfer.	Inspected that formalised procedures are in place for ensuring a valid basis of transfer. Inspected that procedures are up to date. Inspected, by sample test, that documentation confirms a valid basis of transfer in the data processing agreement with the data controller and that transfers have only taken place insofar as this was arranged with the data controller.	No exceptions noted.

Control objective H – Rights of the data subjects

Procedures and controls are complied with to ensure that the data processor can assist the data controller in handing out, correcting, deleting, or restricting information on the processing of personal data to the data subject

Nr.	Twoday control activity	Tests performed by RSM	Result of test
H.1	Written procedures are in place which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects. Inspected that procedures are up to date.	No exceptions noted.
H.2	The data processor has established procedures that, insofar as this was agreed, enable timely assistance to the data controller in handing out, correcting, deleting or restricting or providing information about the processing of personal data to data subjects.	Inspected that the procedures in place for assisting the data controller include detailed procedures for: • Handing out data • Correcting data • Deleting data • Restricting the processing of personal data • Providing information about the processing of personal data to data subjects. Inspected documentation that the systems and databases used support the performance of the relevant detailed procedures.	No exceptions noted.

Control objective I – Managing personal data breaches

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

Nr.	Twoday control activity	Tests performed by RSM	Result of test
I.1	Written procedures are in place which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. Inspected that procedures are up to date.	No exceptions noted.
I.2	The data processor has established the following controls to identify any personal data breaches: • Awareness of employees • Monitoring of network traffic • Follow-up on logging of access to personal data	Inspected that the data processor provides awareness training to the employees in identifying any personal data breaches. Inspected documentation that network traffic is monitored and that anomalies, monitoring alarms, large file transfers, etc. are followed up on. Inspected documentation that logging of access to personal data, including follow-up on repeated attempts to gain access, is followed up on in a timely manner.	No exceptions noted.
I.3	If any personal data breach occurred, the data processor informed the data controller without undue delay after having become aware of such personal data breach at the data processor or a sub-processor.	Inspected that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach. Inquired whether personal data breaches have been identified at the sub-processors.	No exceptions noted. We have noted that there have been no personal data security breaches during the audit period.

Control objective I – Managing personal data breaches

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

Nr.	Twoday control activity	Tests performed by RSM	Result of test
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency. These procedures must contain instructions on descriptions of: • The nature of the personal data breach • Probable consequences of the personal data breach • Measures taken or proposed to be taken to respond to the personal data breach.	Inspected that the procedures in place for informing the data controllers in the event of any personal data breach include detailed instructions for: • Describing the nature of the personal data breach • Describing the probable consequences of the personal data breach • Describing measures taken or proposed to be taken to respond to the personal data breach. • Inspected documentation that the procedures available support that measures are taken to respond to the personal data breach.	No exceptions noted.

The signatures in this document are legally binding. The document is signed with Addo Sign secure digital signature.
The signer's identity is physically registered in the electronic PDF document and shown below.
All times are given in Coordinated Universal Time (UTC).

Signers

 Elias Inderberg Country Managing Director cf108934-c93f-4e9d-a9b0-11d7ea36f540 2026-09-07 14:13:15Z	 Carsten Andersen Business Unit Director 48beff95-a05a-4a66-b244-8d287171b676 2026-09-07 16:27:20Z
 Andreas Moos Head of IT Risk Assurance, RSM Danmark 0303be40-d0bf-4b67-8a20-e59d09e0be9c 2026-09-09 08:49:01Z	 Martin Enderberg Lassen Statsautoriseret Revisor 468a1249-a838-4bbe-a1c8-63a6f30f262d 2026-09-09 09:11:31Z

Documents in the transaction

twoday_ISAE3000_GDPR_2026_assurance report Final.pdf	SHA256: 9a07e1553f4ec4b6252cf7d9df969cd552267b3241f31952ffe3ce3bd578f09f
--	---



The document is digitally signed with the Addo Sign secure signing service. The signature evidence in the document is secured and validated using the mathematical hash value of the original document.

The document is locked for changes and time-stamped with a certificate from a trusted third party. All cryptographic signing proofs are embedded in the PDF document in case they are to be used for validation in the future.

How to verify the authenticity of the document
The document is protected with an Adobe CDS certificate. When the document is opened in Adobe Reader, it will appear to be signed with the Addo Sign signing service.

Addo Sign identification number: 962a3d83-6a34-4a96-a544-51d2f3b70991