Assurance report

# twoday A/S

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with customers using operation of SaaS solutions and consultancy services throughout the period from 1 April 2023 to 31 March 2024

November 2024

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

# Table of contents

# Section 1: twoday A/S' statement

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

twoday A/S uses the following sub-processors: Microsoft, IT Relation A/S and Cloud Factory A/S. This statement does not include control objectives and related controls at twoday A/S' sub-processors. Certain control objectives in the description can only be achieved, if the sub-processor's controls, assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities performed by sub-processors.

Some of the control areas, stated in twoday A/S' description in Section 3 of the operation of SaaS solutions and consultancy services, can only be achieved if the complementary user entity controls with the data controllers are suitably designed and operationally effective with twoday A/S' controls. This assurance report does not include the appropriateness of the design and operational effectiveness of these complementary user entity controls.

twoday A/S confirms that:

a) The accompanying description, Section 3, fairly presents how twoday A/S has processed personal data for data controllers subject to the Regulation throughout the period from 1 April 2023 to 31 March 2024. The criteria used in making this statement were that the accompanying description:

   (i) Presents how twoday A/S' processes and controls were designed and implemented, including:

   - The types of services provided, including the type of personal data processed
   - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete, and restrict processing of personal data
   - The procedures used to ensure that data processing has taken place in accordance with contract, instructions, or agreement with the data controller
   - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality
   - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation
   - The procedures supporting in the event of breach of personal data security that the data controller may report this to the supervisory authority and inform the data subjects
   - The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed
   - Controls that we, in reference to the scope of twoday A/S, have assumed would be implemented by the data controllers and which, if necessary, in order to achieve the control objectives stated in the description, are identified in the description
   - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data

(ii) Includes relevant information about changes in the data processor's operation of SaaS solutions and consultancy services in the processing of personal data during the period from 1 April 2023 to 31 March 2024;

(iii) Does not omit or distort information relevant to the scope of operation of 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 operation of SaaS solutions and consultancy services that the individual data controllers might consider important in their particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were, in our view, suitably designed and operated effectively throughout the period from 1 April 2023 to 31 March 2024 If relevant controls with sub-processors were operationally effective and data controller has performed the complementary user entity controls, assumed in the design of twoday A/S' controls throughout the period from 1 April 2023 to 31 March 2024. The criteria used in making this statement were that:

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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 April 2023 to 31 March 2024.

c) Appropriate technical and organisational safeguards were established and maintained to comply with the agreements with the data controllers, sound data processing practices and relevant requirements for data processors in accordance with the Regulation.

Copenhagen, 15 November 2024
twoday A/S

Lars Engell Berthelsen
Director

# Section 2: Independent auditor's ISAE 3000 assurance report with reasonable assurance on information security and measures pursuant to twoday A/S' data processing agreements with data controllers during the period 1 April 2023 to 31 March 2024

To: twoday A/S and their customers

## Scope

We were engaged to provide assurance about a) twoday A/S' description, Section 3 of the operation of SaaS solutions and consultancy services in accordance with the data processing agreement with data controllers throughout the period from 1 April 2023 to 31 March 2024 and about b+c) the design and operational effectiveness of controls related to the control objectives stated in the Description. twoday A/S uses the following sub-processors: Microsoft, IT Relation A/S and Cloud Factory A/S. This statement does not include control objectives and related controls at twoday A/S' sub-processors. Certain control objectives in the description can only be achieved if the sub-processor's controls, assumed in the design of our controls, are appropriately designed, and operating effectively. The description does not include control activities performed by sub-processors. Some of the control objectives stated in twoday A/S' description in Section 3 of the operation of SaaS solutions and consultancy services, can only be achieved if the complementary user entity controls with the data controller have been appropriately designed and operating effectively with the controls with twoday A/S. The report does not include the appropriateness of the design and operational effectiveness of these complementary user entity controls.

Our opinion is based on reasonable assurance.

## twoday A/S' responsibilities

twoday A/S is responsible for: preparing the Description and the accompanying statement, Section 1, including the completeness, accuracy, and the method of presentation of the Description and statement, providing the services covered by the Description; stating the control objectives; and for the design and implementation of operationally effective controls, to achieve the stated control objectives.

## Grant Thornton's independence and quality control

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

Grant Thornton applies International Standard on Quality Management 1, ISQM 1, requiring that we maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

## Auditor's responsibilities

Our responsibility is to express an opinion on twoday A/S' Description and on the design and operational effectiveness of controls related to the control objectives stated in that Description, based on our procedures.

We conducted our engagement in accordance with International Standard on Assurance Engagements 3000, "Assurance Engagements Other than Audits or Reviews of Historical Financial Information", and additional requirements under Danish audit regulation, to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are appropriately designed and operating effectively.

An assurance engagement to report on the Description, design, and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's

description of its operation of SaaS solutions and consultancy services and about the design and operating effectiveness of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not appropriately designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the Description, the appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data processor and described in Section 1.

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

## Limitations of controls at a data processor

twoday A/S' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the operation of SaaS solutions and consultancy services that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect personal data breaches. Furthermore, the projection of any evaluation of the operating effectiveness to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

## Opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the *Management's statement* Section 1. In our opinion, in all material respects:

(a) The Description fairly presents the operation of SaaS solutions and consultancy services as designed and implemented throughout the period from 1 April 2023 to 31 March 2024;

(b) The controls related to the control objectives stated in the Description were appropriately designed throughout the period from 1 April 2023 to 31 March 2024; to obtain reasonable assurance that the control objectives stated in the Description would be obtained if controls with sub-processors were operating effectively and if data controller has designed and implemented the complementary user entity controls, assumed in the design of twoday A/S' controls throughout the period from 1 April 2023 to 31 March 2024, and

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period from 1 April 2023 to 31 March 2024.

## Description of tests of controls

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

## Intended users and purpose

This report and the description of tests of controls in Section 4 are intended only for data controllers who have used twoday A/S' operation of SaaS solutions and consultancy services who have a sufficient understanding to consider it along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the Regulation have been complied with.

Copenhagen, 15 November 2024

**Grant Thornton**
Godkendt Revisionspartnerselskab

Anders Holmgaard Christiansen
State Authorised Public Accountant

Andreas Moos
Director, CISA, CISM

# Section 3: twoday A/S' description of processing activity for the operation of SaaS solutions and consultancy services

## The company and our performance

We are an international and leading provider of business-critical IT-solutions in the Nordics. An IT-company who provides software development, data- and analytics solutions, consulting services 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 *t*woday Group 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 – through the 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 *t*woday 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.

We 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 digitization of the public sector is one important answer.

## We digitise the Nordics

We continue our long-term effort in digitalising the Nordics. We help both public and private companies to design, develop, modernise, and maintain software. We provide both bespoke solutions and commercial off- the-shelf solutions. Together with our customers, we create increased productivity and growth in the Nordics for the benefit of all of us.

In close collaboration with customers, we develop end-to-end business software and self- service solutions that help customers to improve productivity by digitisation, automation, and integration of business processes. Subsequently we maintain and further develop the solutions as part of the application lifecycle management service to keep the software updated and efficient 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, organise, store, analyse, and visualise 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

*t*woday Group 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 regulations. 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.

## Solutions and service

Solutions and services from *t*woday Group:

- Bespoke solutions and services
- Systems development and project delivery
- Application lifecycle Management
- Business intelligence
- Big data
- Machine learning
- Predictive analytics
- Case & document management
- 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 *t*woday A/S. Agreements are by default based on *t*woday 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, *t*woday ensures that services are fit for purpose of the agreement.

Where *t*woday 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 *t*woday 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. *t*woday A/S does not store data of any EU citizen themselves - all infrastructure related to processing of EU PII is presently located with external hosting partner.

## Personal information

*t*woday A/S has stored:

- Personal information (Name, Address, email, phone etcetera)
- Classified information (CPR, Income)

Categories of data subjects that are used in a DPA

- Pension takers
- Unemployed workers in Denmark (at one time or another)
- Digital Signers
- Pension Brokers
- People in Fishery (employees, ship owners, fishermen)

## Practical deployments

Management in *t*woday Group or *t*woday A/S has approved all procedures, controls, internal tools, and instructions to sub data processors.

Organizationally 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 one-hour meeting where security awareness is presented.

Access to *t*woday 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's rights according to the general risk management process. Furthermore, *t*woday A/S performs every year an analysis and documents all the data where *t*woday A/S is a data controller.

## 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. Subsequently access can only be given if Team Lead approves. Access is also revoked on Team Lead's request and all access (except support) is revoked upon termination of project.

**Procedure for development**
Most of *t*woday A/S' projects are performed at client site where *t*woday 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 *t*woday's Data Protection Counsil for any request, including registered data subjects, for further processing.

## Procedure for security incidents

Security (and privacy) incidents are managed through Incident Management/SOC in *t*woday Group. They are available 24/7 and they are contacted in case of breach. From there they follow a strict procedure to contain, collect information and remedy the situation.

## Sub-processors

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.

## Employees

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

## Significant changes in the period

twoday a/s has not had significant changes during the period from 1 April 2023 to 31 March 2024, regarding our operational services in connection with SaaS and consultancy services.

## Complementary user entity controls with customers

For all our projects, where data is stored outside *t*woday A/S' control – e.g., public projects where data is stored with customers. Thus, it is the customer that is responsible for maintaining the security and privacy for all data stored. It is also the customer that controls the access to data – gives access, audits, and revokes access again. *t*woday A/S follows the procedures given to gain access and follows the DPA that *t*woday A/S has with the customer – *t*woday A/S is still responsible for how its employees act within the systems hosted at the customer when access has been granted.

For a number of projects, *t*woday A/S works together with a third party for the customer. The contract with the third party is with the customer, but *t*woday 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.

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

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

Our test of the functionality has included the control objectives and attached controls, selected by management and which are stated in the control objectives A-I below. Our test has included the controls, we find necessary to establish reasonable assurance for compliance with the articles stated throughout the period from 1 April 2023 to 31 March 2024.

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

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

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

| Method | General description |
|---|---|
| Inquiries | Interview with appropriate personnel at twoday A/S. The interviews have included questions about, how controls are performed. |
| Observation | Observing how controls are performed. |
| Inspection | Review and evaluation of policies, procedures and documentation concerning the performance of controls. This includes reading and assessment of reports and documents in order to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented. Further, it is assessed whether controls are monitored and controlled adequately and with suitable intervals. The effectiveness of the controls during the audit period, is assessed by sample testing. |
| Re-performance | Re-performance of controls to verify that the control is working as assumed. |

**List of control objectives compared to GDPR-articles, ISO 27701, and ISO 27001/2**

Below, control objectives are mapped against the articles in GDPR, ISO 27701 and ISO 270001/2.

Articles and points about main areas are written in bold.

| Control activity | GDPR articles | ISO 27701 | ISO 27001/2:2013 |
|---|---|---|---|
| **A.1** | 5, 26, **28**, 29, 30, 32, 40, 41, 42, 48 | 8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, **8.2.2** | *New scope compared to ISO 27001/2* |
| **A.2** | **28**, 29, 48 | 8.5.5, 6.15.2.2, **6.15.2.2** | 18.2.2 |
| **A.3** | **28** | **8.2.4, 6.15.2.2** | 18.2.2 |
| **B.1** | 31, **32**, 35, 36 | **5.2.2** | 4.2 |
| **B.2** | **32,** 35, 36 | **7.2.5, 5.4.1.2, 5.6.2** | 6.1.2, 5.1, 8.2 |
| **B.3** | **32** | **6.9.2.1** | **12.2.1** |
| **B.4** | 28 stk. 3; litra e, **32; stk. 1** | **6.10.1.1, 6.10.1.2, 6.10.1.3**, 6.11.1.3 | **13.1.2**, 13.1.3, 14.1.3, 14.2.1 |
| **B.5** | 32 | 6.6.1.2, 6.10.1.3 | 9.1.2, 13.1.3, 14.2.1 |
| **B.6** | **32** | **6.6** | 9.1.1, 9.2.5 |
| **B.7** | **32** | **6.9.4** | 12.4 |
| **B.8** | **32** | **6.15.1.5** | 18.1.5 |
| **B.9** | **32** | **6.9.4** | 12.4 |
| **B.10** | **32** | **6.11.3** | 14.3.1 |
| **B.11** | **32** | **6.9.6.1** | 12.6.1 |
| **B.12** | 28, **32** | **6.9.1.2, 8.4** | 12.1.2 |
| **B.13** | **32** | **6.6** | 9.1.1 |
| **B.14** | **32** | **7.4.9** | *New scope compared to ISO 27001/2* |
| **B.15** | **32** | **6.8** | 11.1.1-6 |
| **C.1** | **24** | **6.2** | 5.1.1, 5.1.2 |
| **C.2** | **32, 39** | **6.4.2.2, 6.15.2.1, 6.15.2.2** | 7.2.2, 18.2.1,18.2.2 |
| **C.3** | **39** | **6.4.1.1-2** | 7.1.1-2 |
| **C.4** | 28, 30, **32, 39** | **6.10.2.3**, 6.15.1.1, 6.4.1.2 | 7.1.2, 13.2.3 |
| **C.5** | **32** | **6.4.3.1, 6.8.2.5, 6.6.2.1** | 7.3.1, 11.2.5, 8.3.1 |
| **C.6** | **28,** 38 | **6.4.3.1, 6.10.2.4** | 7,3.1, 13.2.4 |
| **C.7** | **32** | **5.5.3, 6.4.2.2** | 7.2.2, 7.3 |
| **C.8** | **38** | **6.3.1.1, 7.3.2** | 6.1.1 |
| **C.9** | 6, 8, 9, 10, 15, 17, 18, 21, 28, **30**, 32, 44, 45, 46, 47, 48, 49 | 6.12.1.2, 6.15.1.1, 7.2.2, **7.2.8**, 7.5.1, 7.5.2, 7.5.3, 7.5.4, **8.2.6**, 8.4.2, 8.5.2, 8.5.6 | *New scope compared to ISO 27001/2* |
| **D.1** | 6, 11, **13, 14,** 32 | **7.4.5**, **7.4.7**, 7.4.4 | *New scope compared to ISO 27001/2* |
| **D.2** | 6, 11, 13, 14, **32** | **7.4.5**, **7.4.7**, 7.4.4 | *New scope compared to ISO 27001/2* |
| **D.3** | 13, **14** | **7.4.7**, 7.4.4 | *New scope compared to ISO 27001/2* |
| **E.1** | 13, 14, **28,** 30 | **8.4.2, 7.4.7, 7.4.8** | *New scope compared to ISO 27001/2* |
| **E.2** | 13, 14, **28,** 30 | **8.4.2, 7.4.7, 7.4.8** | *New scope compared to ISO 27001/2* |
| **F.1** | 6, 8, 9, 10, 17, 18, 22, 24, 25, 28, **32,** 35, 40, 41, 42 | 5.2.1, **7.2.2**, **7.2.6**, 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7 | 15 |
| **F.2** | **28** | **8.5.7** | 15 |
| **F.3** | **28** | **8.5.8**, 8.5.7 | 15 |
| **F.4** | **33, 34** | **6.12.1.2** | 15 |
| **F.5** | **28** | **8.5.7** | 15 |
| **F.6** | **33, 34** | **6.12.2** | 15.2.1-2 |
| **G.1** | 15, 30, **44, 45,** 46, 47, 48, 49 | **6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, **8.5.1**, 8.5.2, 8.5.3 | 13.2.1, 13.2.2 |
| **G.2** | 15, 30, **44, 45,** 46, 47, 48, 49 | **6.10.2.1, 7.5.1,** 7.5.2, 7.5.3, 7.5.4, **8.4.2,** 8.5.2, 8.5.3 | 13.2.1 |
| **G.3** | 15, 30, **44, 45,** 46, 47, 48, 49 | **6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, 8.5.3 | 13.2.1 |
| **H.1** | 12, **13, 14,** 15, 20, 21 | **7.3.5, 7.3.8, 7.3.9** | *New scope compared to ISO 27001/2* |
| **H.2** | 12, **13, 14,** 15, 20, 21 | **7.3.5, 7.3.8, 7.3.9** | *New scope compared to ISO 27001/2* |
| **I.1** | **33, 34** | **6.13.1.1** | 16.1.1-5 |
| **I.2** | **33, 34**, 39 | 6.4.2.2, **6.13.1.5, 6.13.1.6** | 16.1.5-6 |
| **I.3** | **33, 34** | **6.13.1.4** | 16.1.5 |
| **I.4** | **33, 34** | **6.13.1.4,** 6.13.1.6 | 16.1.7 |

## Control objective A - Instructions regarding processing of personal data

Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistently with the data processing agreement entered into.

| *No.* | *twoday A/S' control activity* | *Test performed by Grant Thornton* | *Result of test* |
|---|---|---|---|
| A.1 | Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | We have inspected that formalised procedures exist to ensure that personal data are only processed according to instructions.<br>We have inspected that the procedures include a requirement to assess at least once a year the need for updates, including in case of changes in the data controller's instructions or changes in the data processing.<br>We have inspected that procedures are up to date. | No deviations noted. |
| A.2 | The data processor only processes personal data stated in the instructions from the data controller. | We have inspected that management ensures that personal data are only processed according to instructions.<br>We have inspected that a sample of personal data processing operations are conducted consistently with instructions. | No deviations noted. |
| A.3 | The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions. | We have inspected that formalised procedures exist ensuring verification that personal data are not processed against the Regulation or other legislation.<br>We have inspected that procedures are in place for informing the data controller of cases where the processing of personal data is evaluated to be against legislation.<br>We have inspected that the data controller was informed in cases where the processing of personal data was evaluated to be against legislation. | We have been informed that the data processor has not received instructions which, in the data processor's opinion, contravene the data protection regulation or data protection provisions in other EU law or the national law of the Member States.<br>No deviations noted. |

## Control objective B - Technical measures

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

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

## Control objective B - Technical measures

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

| *No.* | *twoday A/S' control activity* | *Test performed by Grant Thornton* | *Result of test* |
|---|---|---|---|
| B.5 | Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. | We have inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.<br><br>We have inspected network diagrams and other network documentation to ensure appropriate segmentation. | No deviations noted. |
| B.6 | Access to personal data is isolated to users with a work-related need for such access. | We have inspected that formalised procedures are in place for restricting users' access to personal data.<br><br>We have inspected that formalised procedures are in place for following up on users' access to personal data being consistent with their work-related need.<br><br>We have inspected that access is restricted to the employees' work-related need for access to systems and databases. | No deviations noted. |
| B.7 | For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. | We have inspected that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.<br><br>We have inspected that a sample of alarms were followed up on and that the data controllers were informed thereof as appropriate. | No deviations noted. |
| B.8 | Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email. | We have inspected that formalised procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognised algorithm.<br><br>We have inspected that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email. | No deviations noted. |

## Control objective B - Technical measures

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

| *No.* | *twoday A/S' control activity* | *Test performed by Grant Thornton* | *Result of test* |
|---|---|---|---|
| B.9 | Logging has been established in systems, databases, and networks.<br><br>Log data are protected against manipulation, technical errors and are reviewed regularly. | We have inspected that logging of user activities in systems, databases or networks that are used to process or transmit personal data has been configured and activated.<br><br>We have inspected that user activity data collected in logs are protected against manipulation or deletion.<br><br>We have, by sample test, inspected that the content of a sample of log files is as expected compared to the setup and that documentation exists regarding the follow-up performed and the response to any security incidents.<br><br>We have, by sample test, inspected that documentation exists for the follow-up performed for activities carried by system administrators and others holding special rights. | No deviations noted. |
| B.11 | The technical measures established are tested on a regular basis in vulnerability scans. | We have inspected that formalised procedures exist for regularly testing technical measures, including for performing vulnerability scans.<br><br>We have inspected samples that documentation exists regarding regular testing of the technical measures established.<br><br>We have inspected that no significant deviations or weaknesses in the technical measures have been identified. | No deviations noted. |
| B.12 | Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches. | We have inspected that formalised procedures exist for handling changes to systems, databases, or networks, including handling of relevant updates, patches, and security patches. | twoday has implemented a new change management procedure after the end of the assurance period where the history of changes deployed to production environments are not saved for audit purposes. Therefore, we have not been able to test the control.<br><br>No further deviations noted. |

## Control objective B - Technical measures

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

| *No.* | *twoday A/S' control activity* | *Test performed by Grant Thornton* | *Result of test* |
|---|---|---|---|
| B.13 | A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need. | We have inspected that formalised procedures exist for granting and removing users' access to systems and databases using to process personal data.<br>We have inspected that documentation exists that user accesses granted are evaluated and authorised on a regular basis – and at least once a year. | No deviations noted. |
| B.14 | Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication. | We have inspected that users' access to processing personal data that involve a high risk for the data subjects can only take place by using two-factor authentication. | No deviations noted. |
| B.15 | Physical access safeguards have been established so as to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed. | We have inspected that formalised procedures exist to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed.<br>We have inspected documentation that, throughout the assurance period, only authorised persons have had physical access to premises at which personal data are stored and processed. | No deviations noted. |

## Control objective C - Organisational measures

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

| *No.* | *twoday A/S' control activity* | *Test performed by Grant Thornton* | *Result of test* |
|---|---|---|---|
| C.1 | Management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The IT security policy is based on the risk assessment performed.<br><br>Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated. | We have inspected that an information security policy exists that Management has considered and approved within the past year.<br><br>We have inspected documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees. | No deviations noted. |
| C.2 | Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into. | We have inspected documentation of management's assessment that the information security policy generally meets the requirements for safeguards and the security of processing in the data processing agreements entered into.<br><br>We have, by sample test, inspected that the requirements in data processing agreements are covered by the requirements of the information security policy for safeguards and security of processing. | No deviations noted. |
| C.4 | Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data. | We have, by sample test, inspected that employees appointed during the assurance period have signed a confidentiality agreement.<br><br>We have, by sample test, inspected that employees appointed during the assurance period have been introduced to:<br><br>• Information security policy.<br>• Procedures for processing data and other relevant information. | No deviations noted. |

## Control objective C - Organisational measures

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

| *No.* | *twoday A/S' control activity* | *Test performed by Grant Thornton* | *Result of test* |
|---|---|---|---|
| C.5 | For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned. | We have inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal and that assets such as access cards, computers, mobile phones, etc. are returned.<br><br>We have, by sample test, inspected that rights have been deactivated or terminated and that assets have been returned for employees resigned or dismissed during the assurance period. | Documentation is not available showing that 3 out of 5 terminated employees have had their access rights cancelled in a timely manner.<br><br>We have been informed that the reason for lack of documentation is due to the retention time in Azure.<br><br>No further deviations noted. |
| C.6 | Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers. | We have inspected that formalised procedures exist to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality.<br><br>We have, by sample test, inspected that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality for employees resigned or dismissed during the assurance period. | 4 out of 5 samples of terminated employees have not been informed about continued validity of confidentiality.<br><br>No further deviations noted. |
| C.7 | Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data. | We have inspected that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data.<br><br>We have inspected documentation that all employees who have either access to or process personal data have completed the awareness training provided. | No deviations noted. |

## Control objective D - Return and deletion of personal data

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

| *No.* | *twoday A/S' control activity* | *Test performed by Grant Thornton* | *Result of test* |
|---|---|---|---|
| D.1 | Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller.<br><br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | We have inspected that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller.<br><br>We have inspected that the procedures are up to date. | No deviations noted. |
| D.2 | Specific requirements have been agreed with respect to the data processor's storage periods and deletion routines. | We have inspected that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines.<br><br>We have, by sample test, inspected that documentation exists of personal data being stored in accordance with the agreed storage periods in data processing agreements.<br><br>We have, by sample test, inspected that documentation exists that personal data are deleted in accordance with the agreed deletion routines in data processing agreements. | No deviations noted. |
| D.3 | Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been:<br><br>• Returned to the data controller; and/or<br>• Deleted if this is not in conflict with other legislation. | We have inspected that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data.<br><br>We have inspected that methods to delete personal data in accordance with the agreed storage periods have been implemented.<br><br>We have inquired into whether data processing has ceased within the past year. | We have been informed that no data processing has ceased during the period.<br><br>No deviations noted. |

## Control objective E – Storage of personal data

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

| *No.* | *twoday A/S' control activity* | *Test performed by Grant Thornton* | *Result of test* |
|---|---|---|---|
| E.1 | Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller.<br><br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | We have inspected that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements.<br><br>We have inspected that the procedures are up to date. | No deviations noted. |
| E.2 | Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller. | We have inspected that the data processor has a complete and updated list of processing activities stating localities, countries, or regions.<br><br>We have, by sample test, inspected that documentation exists that the processing of data, including the storage of personal data, takes place only in the localities stated in the data processing agreement – or otherwise as approved by the data controller. | No deviations noted. |

## Control objective F – Use of sub-processors

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

| *No.* | *twoday A/S' control activity* | *Test performed by Grant Thornton* | *Result of test* |
|---|---|---|---|
| F.1 | Written procedures exist which include requirements for the data processor when using sub-processors, including requirements for sub-data processing agreements and instructions.<br><br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | We have inspected that formalised procedures are in place for using sub-processors, including requirements for sub-data processing agreements and instructions.<br><br>We have inspected that procedures are up to date. | The written procedure for use of sub-processors has not been updated.<br><br>No further deviations noted. |
| F.2 | The data processor only uses sub-processors to process personal data that have been specifically or generally approved by the data controller. | We have inspected that the data processor has a complete and updated list of sub-processors used.<br><br>We have, by sample test, inspected that documentation exists that the processing of data by the sub-processor is stated in the data processing agreements – or otherwise as approved by the data controller. | No deviations noted. |
| F.3 | When changing the generally approved sub-processors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the data processor. When changing the specially approved sub-processors used, this has been approved by the data controller. | We have inspected that formalised procedures are in place for informing the data controller when changing the sub-processors used.<br><br>We have inspected documentation that the data controller was informed when changing the sub-processors used throughout the assurance period. | We have been informed that there have been no changes in the use of sub-processors during the audit period.<br><br>No deviations noted. |
| F.4 | The data processor has subjected the sub-processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller. | We have inspected the existence of signed sub-data processing agreements with sub-processors used, which are stated on the data processor's list.<br><br>We have, by sample test, inspected that sub-data processing agreements include the same requirements and obligations as are stipulated in the data processing agreements between the data controllers and the data processor. | No deviations noted. |

## Control objective F – Use of sub-processors

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

| *No.* | *twoday A/S' control activity* | *Test performed by Grant Thornton* | *Result of test* |
|---|---|---|---|
| F.5 | The data processor has a list of approved sub-processors. | We have inspected that the data processor has a complete and updated list of sub-processors used and approved.<br><br>We have inspected that, as a minimum, the list includes the required details about each sub-processor. | No deviations noted. |
| F.6 | Based on an updated risk assessment of each sub-processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the sub-processor. | We have inspected that formalised procedures are in place for following up on processing activities at sub-processors and compliance with the sub-data processing agreements.<br><br>We have inspected documentation that each sub-processor and the current processing activity at such processor are subjected to risk assessment.<br><br>We have inspected documentation that technical and organisational measures, security of processing at the sub-processors used, third countries' bases of transfer and similar matters are appropriately followed up on.<br><br>We have inspected documentation that information on the follow-up at sub-processors is communicated to the data controller so that such controller may plan an inspection. | No deviations noted. |

## Control objective G – Transfer of personal data to third countries

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

| *No.* | *twoday A/S' control activity* | *Test performed by Grant Thornton* | *Result of test* |
|---|---|---|---|
| G.1 | Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.<br><br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | We have inspected that formalised procedures exist to ensure that personal data are only transferred to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. | No deviations noted. |
| G.2 | The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller. | We have inquired whether the data processor has transferred personal data to third countries or international organisations. | We have been informed that no transfers of personal data to third countries or international organisations have occurred in the audit period.<br><br>No deviations noted. |
| G.3 | As part of the transfer of personal data to third countries or international organisations, the data processor assessed and documented the existence of a valid basis of transfer. | We have inquired whether the data processor has transferred personal data to third countries or international organisations. | We have been informed that no transfers of personal data to third countries or international organisations have occurred in the audit period.<br><br>No deviations noted. |

## Control objective H – Rights of the data subjects

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

| *No.* | *twoday A/S' control activity* | *Test performed by Grant Thornton* | *Result of test* |
|---|---|---|---|
| H.1 | Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects.<br><br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | We have inspected that formalised procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects.<br><br>We have inspected that procedures are up to date. | No deviations noted. |
| H.2 | The data processor has established procedures as far as this was agreed that enable timely assistance to the data controller in handing out, correcting, deleting, or restricting or providing information about the processing of personal data to data subjects. | We have inspected that the procedures in place for assisting the data controller include detailed procedures for:<br><br>• Handing out data<br>• Correcting data<br>• Deleting data<br>• Restricting the processing of personal data<br>• Providing information about the processing of personal data to data subjects.<br><br>We have inquired whether the data processor has received requests from the data controller in relation to the rights of the data subjects.<br><br>We have inspected documentation that the systems and databases used, support the performance of the relevant detailed procedures. | We have been informed that the data processor has not received requests from the data controller in relation to the data subjects' rights.<br><br>No deviations noted. |

## Control objective I – Managing personal data breaches

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

| *No.* | *twoday A/S' control activity* | *Test performed by Grant Thornton* | *Result of test* |
|---|---|---|---|
| I.1 | Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches.<br><br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | We have inspected that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches.<br><br>We have inspected that procedures are up to date. | No deviations noted. |
| I.2 | The data processor has established controls for identification of possible personal data breaches. | We have inspected that the data processor provides awareness training to the employees in identifying any personal data breaches.<br><br>We have inspected documentation that network traffic is monitored and that anomalies, monitoring alarms, large file transfers, etc. are followed up on.<br><br>We have inspected documentation that logging of access to personal data, including follow-up on repeated attempts to gain access, is followed up on, on a timely basis. | No deviations noted. |
| I.3 | If any personal data breach occurred, the data processor informed the data controller without undue delay after having become aware of such personal data breach at the data processor or a sub-processor. | We have inspected that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach.<br><br>We have inspected that the data processor has included any personal data breaches at sub-processors in the data processor's list of security incidents. | No deviations noted. |

| Control objective I – Managing personal data breaches<br>Procedures and controls are complied with to ensure that any personal data breaches are responded to in accordance with the data processing agreement entered into. | | | |
|---|---|---|---|
| *No.* | *twoday A/S' control activity* | *Test performed by Grant Thornton* | *Result of test* |
| I.4 | The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency:<br>• Nature of the personal data breach<br>• Probable consequences of the personal data breach<br>• Measures taken or proposed to be taken to respond to the personal data breach. | We have inspected that the procedures in place for informing the data controllers in the event of any personal data breach include detailed procedures for:<br>• Describing the nature of the personal data breach<br>• Describing the probable consequences of the personal data breach<br>• Describing measures taken or proposed to be taken to respond to the personal data breach.<br>We have inspected documentation that, when a personal data breach occurred, measures were taken to respond to such breach. | No deviations noted. |

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet med Addo Sign sikker digital underskrift.
Underskrivers identitet er fysisk registreret i det elektroniske PDF dokument og vist herunder.
Alle tider er angivet i Universaltid (UTC).

## Underskrivere

***Lars Engell Berthelsen***
*Managing Director*
*d633e749-7580-4677-890b-83600de08951* *2024-11-15 16:38:36Z*

***Andreas Moos***
*Director | IT Risk Assurance & Advisory Services*
*eace5ed6-cfa7-4d9e-b982-120d10f47204* *2024-11-15 16:52:07Z*

***Anders Holmgaard Christiansen***
*Partner*
*250abf98-7048-42a1-8db3-222c9125bb0e* *2024-11-17 19:02:09Z*

## Dokumenter i transaktionen

twoday - ISAE 3000-II - GDPR - 2024 - Assurance Report.pdf *SHA256:*
*c114e37d7d478ebdfe0471a8206b7ccd0705c1c34755b4d25fffb33b229648fe*