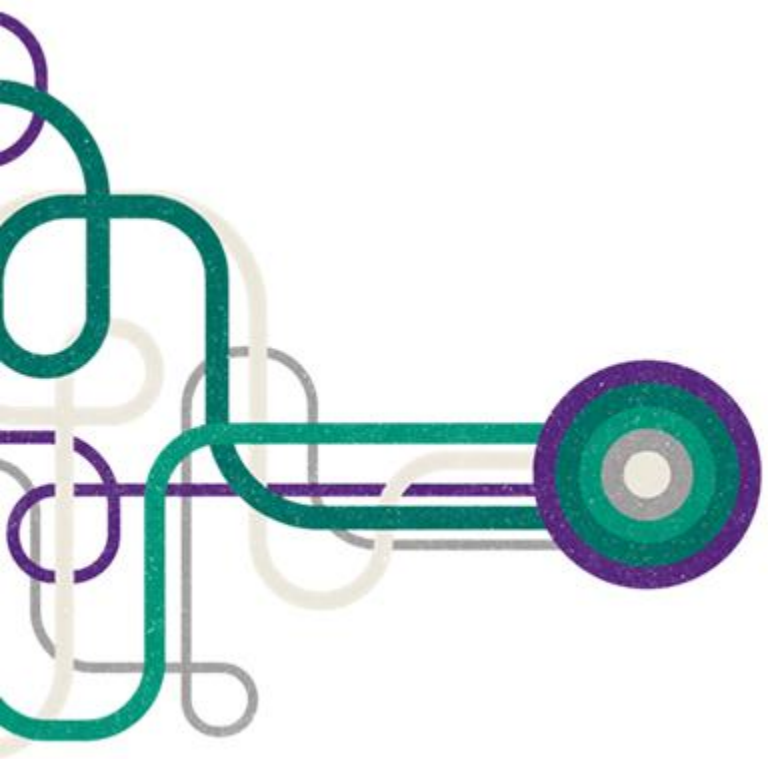
Grant Thornton

An instinct for growth™



# Independent auditor's ISAE 3000 assurance report on internal controls regarding data protection and processing of personal data on the 1st of January 2020 to 31st of December 2020 for

## Sentia Denmark A/S

CVR nr: 10 00 81 23

# Table of Content



**Symbol**

- Our tests have not resulted in any material deviations
- Some weaknesses have been identified in the controls
- Critical weaknesses or deficiencies or have been identified

# 1. Management's statement

Sentia Denmark A/S processes personal data for data controllers in accordance with the data processing agreements on managed private and public cloud solutions and data processing with data controllers.

The accompanying description has been prepared for data controllers, who has used managed private and public cloud solutions and data processing offered by Sentia, 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.

Sentia Denmark A/S confirms that:

a) The accompanying description, section 3, fairly presents controls on the managed private and public cloud solutions and data processing where personal data is processed for data controllers subject to the Regulation throughout the period 1st of January 2020 to 31st of December 2020. The criteria used in making this statement were that the accompanying description:

   i. Presents how cloud based operating platform was 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, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;
      - Controls that we, in reference to the scope of the cloud based operating platform , 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;

# 1. Management's statement (continued)

ii. Includes relevant information about changes in the Data Processor's managed private and public cloud solutions and data processing in the processing of personal data throughout the period 1st of January 2020 to 31st of December 2020;

iii. Does not omit or distort information relevant to the scope of managed private and public cloud solutions and data processing 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 managed private and public cloud solutions and data processing 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 suitably designed and operated effectively throughout the period 1st of January 2020 to 31st of December 2020. 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 persons who have the appropriate competence and authority, throughout the period 1st of January 2020 to 31st of December 2020.

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.

Herlev, 22nd of January 2021

Lyskær 3A, 2730 Herlev

CVR-nr: 10 00 81 23

Jakob Høholdt

Managing Director, Sentia Denmark A/S

# 2. Independent auditor's report

**Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with Sentia Denmark's clients.**

To: Management of Sentia Denmark A/S and data controllers, receiving data processing services from Sentia Denmark A/S.

## Scope

We were engaged to provide assurance about Sentia Denmark A/S' description on page 7-8 of managed private and public cloud solutions and data processing ("Description") in accordance with the data processing agreement with Sentia Denmark A/S' clients throughout the period 1st of January 2020 to 31st of December 2020 the and about the design and operating effectiveness of controls related to the control objectives stated in the description. We express reasonable assurance in our conclusion.

## Sentia Denmark's responsibilities

Sentia Denmark A/S is responsible for: preparing the description in section 3 and the accompanying statement in 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 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 of the Code of Ethics for Professional Accountants issued by FSR - Danish Auditors (Code of Ethics for Professional Accountants), which are based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional conduct.

Grant Thornton is subject to the International Standard on Quality Control (ISQC 1) and accordingly uses and maintains 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 Sentia Denmark A/S' description and on 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 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 managed private and public cloud solutions and data processing 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 3.

# 2. Independent auditor's report (continued)

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 controller

Sentia Denmark 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 managed private and public cloud solutions and data processing 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. In our opinion, in all material respects:

a) The description fairly presents managed private and public cloud solutions and data processing as designed and implemented throughout the period 1st of January 2020 to 31st of December 2020.

b) The controls related to the control objectives stated in the description were appropriately designed throughout the period 1st of January 2020 to 31st of December 2020; 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 1st of January 2020 to 31st of December 2020.

### 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 on page 9 - 36 are intended only for data controllers who have used Sentia Denmark's managed private and public cloud solutions and data processing, 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, 22nd of January 2021

**Grant Thornton**
State authorized public accountants
CVR-nr. 34 20 99 36

Jacob Helly Juell-Hansen
State authorized Public accountant

Anders Grønning-Kjærgaard
Director, Head of IT Audit & Advisory

# 3. Description of processing of personal data

### 3.1 Description of personal data processing by Sentia

Sentia Denmark A/S (hereinafter ´Sentia´) is the leading provider of managed private and public cloud solutions and data processing.

As a data processor or data sub-processor for managed cloud solutions and data processing, Sentia has implemented Data Processing Agreements (DPA), with our customers as data controllers. Data processing is implemented according to customer instructions.

The following description refers to the relevant articles of the General Data Protection Regulation which are included in this statement.

A. Compliance with instructions (Articles 5, 6, 9, 10 and 28)

Sentia processes personal data solely under instructions from the data controller. Sentia safeguards this principle by instructing all employees to do so, based on guidelines on the matter included in a personal data policy, and the registration of customer instructions through DPA. Sentia implement updates to the DPA and instructions based on enquiries from the data controller.

Sentia ensures the lawfulness of the personal data processing by concluding DPA, including instructions.

Sentia immediately notifies the data controller if a processing or instructions is in violation with the data protection regulation.

B. Technical measures (Articles 24, 32 and 35)

Sentia continually maintains risk management of processes regarding personal data among others for our customers, as data controllers.

Sentia has according to contracts with data controller, implemented technical measures that ensures adequate security in accordance with the risk management in ISO 27001:2013.

C. Organizational measures (Articles 25 and 32)

Sentia has implemented policies for information security and processing of personally identifiable information. Sentia has ensured that these policies do not conflict with data processing agreements which are implemented in Sentia. All employees at Sentia are subject to confidentiality.

Sentia has implemented formal onboarding and offboarding procedures as well as frequent information security awareness training.

D. Deletion and return of personal data to data controller (Article 32)

Sentia deletes personal data by agreement / instruction of the data controller, based on retention period and termination of agreement for data processing. Data is returned to the data controller according to exit agreement.

E. Records of processing (Article 30)

Sentia stores personal data according to the data processing agreement with the data controller. This encompasses storage at locations agreed by the data controller. Locations are by default within EU.

F. Sub-data processors (Article 28)

Sentia only uses sub-data processors according to agreement with the data controller, documented in the data processing agreement. Sentia conducts at least yearly control of sub-data processors. Sentia informs data controller about changes in sub-data processors in timely manner. Sentia ensures that sub-data processors live up to the same requirements as agreed between the data controller and Sentia. Sentia maintains an overview of sub-data processors.

# 3. Description of processing of personal data (continued)

G. Transfer to third countries (Article 44)

Sentia transfers only personal data to third party countries if the data controller instructs Sentia to do it. It is the data controller's responsibility to ensure valid basis for transfer to third countries.

H. Right of the registered persons (data subjects) (Articles 15, 16, 17, 18 and 19)

If requests are sent to Sentia they will be forwarded to the data controller. Sentia supports the data controller, in case of requests from data subjects.

I. Personal data breach management (Articles 33 and 34).

Sentia has established a process for the notification of personal data breach to the data controller.

In case of a personal data breach under the responsibility of Sentia, a process for how to handle this has been implemented to ensure reporting to the data controller in timely manner.

Sentia has established a process to assist the data controller in handling data breaches including contact to relevant authorities.

### 3.2 Complementary controls of data controllers

When concluding a DPA, the data controller must ensure that the following has been documented:

- Clarifications/additions to the DPA
- Categories of personal data
- Specific instructions

If, at any time, changes are made to the instructions or categories of personal data, the data controller must report this to gdpr.dk@sentia.com

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

### 4.1 Purpose and scope

We have conducted our engagement in accordance with ISAE 3000, Assurance engagements other than audits or reviews of historical financial information and additional requirements under Danish audit regulation.

Our testing of the design, implementation and functionality of the controls included the control objectives and related control activities selected by Management and listed in the rest of section 4. Any other control objectives, related controls and controls at the affiliated enterprises are not covered by our test activities.

Our operating effectiveness testing included the control activities deemed necessary to obtain reasonable assurance that the stated control activities were achieved throughout the period 1st of January 2020 to 31st of December 2020.

### 4.2 Test activities performed

The test activities performed when determining the operating effectiveness of the controls are described below.

| Metode | General description |
|---|---|
| Inquiries | Inquiry of appropriate personnel. Inquiries have included how the controls are performed. |
| Observation | We have 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. |
| Repetition of the control | Repeat the relevant control. We have repeated the execution of the control to verify that the control functions as assumed. |

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

## Compliance with instruction (control objective A)

| **Control objective:** **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.** | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditors*** | ***Result of auditor's test*** |
| A.1 | Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available.<br><br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | Checked by way of inspection that formalised procedures exist to ensure that personal data are only processed according to instructions.<br><br>Checked by way of inspection 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><br>Checked by way of inspection that procedures are up to date. | Our tests have not resulted in any material deviations. |
| A.2 | The data processor only processes personal data stated in the instructions from the data controller. | Checked by way of inspection that Management ensures that personal data are only processed according to instructions.<br><br>Checked by way of inspection of a sample of seven personal data processing operations that these are conducted consistently with instructions. | Our tests have not resulted in any material deviations. |

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

## Compliance with instruction (control objective A) – continued

| Control objective: 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. | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditors*** | ***Result of auditor's test*** |
| 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. | Checked by way of inspection that formalised procedures exist ensuring verification that personal data are not processed against the Regulation or other legislation.<br><br>Inquired 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><br>Inquired whether the data controller was informed in cases where the processing of personal data was evaluated to be against legislation. | We have been informed that Sentia Denmark A/S has not had cases where they have received instructions that infringe the Regulation or other European Union or member state data protection legislation.<br><br>Our tests have not resulted in any material deviations. |

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

## Technical measures to safeguard relevant security (control objective B)

| **Control objective:**<br>**Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.** | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's test*** |
| B.1 | Written procedures exist which include a requirement that safeguards agreed upon 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. | Checked by way of inspection that formalised procedures exist to ensure establishment of the safeguards as agreed.<br><br>Checked by way of inspection that procedures are up to date.<br><br>Checked by way of inspection of a sample of six data processing agreements that the safeguards agreed have been established. | Our tests have not resulted in any material deviations. |

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

## Technical measures to safeguard relevant security (control objective B)

| **Control objective:**<br>**Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.** | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's test*** |
| 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. | Checked by way of inspection 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>Checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data.<br><br>Checked by way of inspection that the data processor has implemented the technical measures ensuring an appropriate level of security consistent with the risk assessment.<br><br>Checked by way of inspection that the data processor has implemented the safeguards agreed upon with the data controller. | Our tests have not resulted in any material deviations. |

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

## Technical measures to safeguard relevant security (control objective B) - continued

| **Control objective:**<br>**Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.** | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's test*** |
| 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. | Checked by way of inspection that, for the systems and databases used in the processing of personal data, antivirus software has been installed.<br><br>Checked by way of inspection that antivirus software is up to date. | Our tests have not resulted in any material deviations. |
| B.4 | External access to systems and databases used in the processing of personal data takes place through a secured firewall. | Checked by way of inspection that external access to systems and databases used in the processing of personal data takes place only through a secured firewall.<br><br>Checked by way of inspection that the firewall has been configured in accordance with the relevant internal policy. | Our tests have not resulted in any material deviations. |
| 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.<br><br>Inspected network diagrams and other network documentation to ensure appropriate segmentation. | Our tests have not resulted in any material deviations. |

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

## Technical measures to safeguard relevant security (control objective B) - continued

| Control objective: Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's test*** |
| B.6 | Access to personal data is isolated to users with a work-related need for such access. | Checked by way of inspection that formalised procedures are in place for restricting users' access to personal data.<br><br>Checked by way of inspection that formalised procedures are in place for following up on users' access to personal data being consistent with their work-related need.<br><br>Checked by way of inspection that the technical measures agreed support retaining the restriction in users' work-related access to personal data.<br><br>Checked by way of inspection of a sample of three users' access to systems and databases that such access is restricted to the employees' work-related need. | Our tests have not resulted in any material deviations. |

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

## Technical measures to safeguard relevant security (control objective B) - continued

| **Control objective:**<br>**Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.** | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's test*** |
| B.7 | For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. This monitoring comprises:<br>• Availability<br>• Capacity<br>• Incidents | Checked by way of inspection that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.<br>Checked that alarms were followed up on and that the data controllers were informed thereof as appropriate. | Our tests have not resulted in any material deviations. |

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

## Technical measures to safeguard relevant security (control objective B) - continued

| Control objective: Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's test*** |
| B.8 | Logging of the following matters has been established in systems, databases and networks:<br>• Activities performed by system administrators and others holding special rights;<br>• Security incidents comprising:<br>o Changes in log setups, including disabling of logging;<br>o Changes in users' system rights<br>o Failed attempts to log on to systems, databases or networks;<br>Logon data are protected against manipulation and technical errors and are reviewed regularly. | Checked by way of inspection that formalised procedures exist for setting up logging of user activities in systems, databases or networks that are used to process and transmit personal data, including review of and follow-up on logs.<br><br>Checked by way of inspection that user activity data collected in logs are protected against manipulation or deletion.<br><br>Checked that the content 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>Checked that documentation exists regarding the follow-up performed for activities carried by system administrators and others holding special rights. | Our tests have not resulted in any material deviations. |

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

## Technical measures to safeguard relevant security (control objective B) - continued

| Control objective: Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's test*** |
| B.9 | The technical measures established are tested on a regular basis in vulnerability scans and penetration tests. | Checked by way of inspection that formalised procedures exist for regularly testing technical measures, including for performing vulnerability scans and penetration tests.<br><br>Checked by way of inspection of samples that documentation exists regarding regular testing of the technical measures established.<br><br>Checked by way of inspection that any deviations or weaknesses in the technical measures have been responded to in a timely and satisfactory manner and communicated to the data controllers as appropriate. | Our tests have not resulted in any material deviations. |
| B.10 | Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches. | Checked by way of inspection that formalised procedures exist for handling changes to systems, databases or networks, including handling of relevant updates, patches and security patches.<br><br>Checked by way of inspection of extracts from technical security parameters and setups that systems, databases or networks have been updated using agreed changes and relevant updates, patches and security patches. | Our tests have not resulted in any material deviations. |

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

## Technical measures to safeguard relevant security (control objective B) - continued

| Control objective: Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's test*** |
| B.11 | 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. | Checked by way of inspection that formalised procedures exist for granting and removing users' access to systems and databases using to process personal data.<br><br>Checked by way of inspection of a sample of two employees' access to systems and databases that the user accesses granted have been authorised and that a work-related need exists.<br><br>Checked by way of inspection of a sample of one resigned or dismissed employee that access to systems and databases was deactivated or removed on a timely basis.<br><br>Checked by way of inspection that documentation exists that user accesses granted are evaluated and authorized on a regular basis – and at least once a year. | Our tests have not resulted in any material deviations. |

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

## Technical measures to safeguard relevant security (control objective B) - continued

| Control objective:<br>Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's test*** |
| B.12 | 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. | Checked by way of inspection that formalised procedures exist to ensure that two-factor authentication is applied in the processing of personal data that involves a high risk for the data subjects. | Our tests have not resulted in any material deviations. |
| B.13 | 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. | Checked by way of inspection 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><br>Checked by way of inspection of documentation that, throughout the assurance period, only authorized persons have had physical access to premises and data centers at which personal data are stored and processed. | Our tests have not resulted in any material deviations. |

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

## Organisational measures to safeguard relevant security (control objective C)

| **Control objective:**<br>**Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.** | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's 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. | Checked by way of inspection that an information security policy exists that Management has considered and approved within the past year.<br><br>Checked by way of inspection of documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees. | Our tests have not resulted in any material deviations. |
| 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 safeguards and the security of processing in the data processing agreements entered into.<br><br>Checked by way of inspection of a sample of seven data processing agreements that the requirements in these agreements are covered by the requirements of the information security policy for safeguards and security of processing. | Our tests have not resulted in any material deviations. |

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

## Organisational measures to safeguard relevant security (control objective C) – continued

| **Control objective:**<br>**Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.** | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's test*** |
| C.3 | The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant:<br>• Multiple interviews;<br>• References from prior employees;<br>• Certificates of criminal record. | Checked by way of inspection that formalized procedures are in place to ensure screening of the data processor's employees as part of the employment process.<br>Checked by way of inspection of a sample of seven data processing agreements that the requirements therein for screening employees are covered by the data processor's screening procedures.<br>Checked by way of inspection of four employees appointed during the assurance period that documentation exists of the screening having comprised:<br>• Multiple interviews;<br>• References from prior employees;<br>• Certificates of criminal record. | Our tests have not resulted in any material deviations. |

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

## Organisational measures to safeguard relevant security (control objective C) – continued

| Control objective: Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's test*** |
| C.4 | Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data. | Inspected that all employee contracts have clauses regarding confidentiality and are signed upon employment.<br>Inspected that employees have been introduced to:<br>• Information security policy;<br>• Procedures for processing data and other relevant information. | Our tests have not resulted in any material deviations. |
| 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.<br>Checked by way of inspection of four employees resigned or dismissed during the assurance period that rights have been deactivated or terminated and that assets have been returned. | Our tests have not resulted in any material deviations. |

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

## Organisational measures to safeguard relevant security (control objective C) – continued

| Control objective: Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's test*** |
| 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 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. | Our tests have not resulted in any material deviations. |
| 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. | Checked by way of inspection that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data.<br><br>Inspected documentation that all employees who have either access to or process personal data have completed the awareness training provided. | Our tests have not resulted in any material deviations. |

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

## Deleting or returning personal data (control objective D)

| **Control objective:** **Procedures and controls are complied with to ensure that personal data can be deleted or returned if arrangements are made with the data controller to this effect.** | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's 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. | Checked by way of inspection that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller.<br><br>Checked by way of inspection that the procedures are up to date. | Our tests have not resulted in any material deviations. |
| D.2 | The following specific requirements have been agreed with respect to the data processor's storage periods and deletion routines:<br>• Agreements on retention periods for backup is stated in service agreements with customers. Additional deletion is only performed upon instruction from the customer. | Checked by way of inspection that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines.<br><br>Inspected that backup is stored according to agreed retention periods and that changes in backup is handled through the change management process. | Our tests have not resulted in any material deviations. |

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

## Deleting or returning personal data (control objective D) – continued

| Control objective:<br>Procedures and controls are complied with to ensure that personal data can be deleted or returned if arrangements are made with the data controller to this effect. | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's test*** |
| 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>• Returned to the data controller; and/or<br>• Deleted if this is not in conflict with other legislation. | Checked by way of inspection that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data.<br>Inspected one terminated data processing sessions during the assurance period that documentation exists that the agreed deletion or return of data has taken place. | Our tests have not resulted in any material deviations. |

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

## Storage of personal data (control objective E)

| **Control objective:**<br>**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.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's 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. | Checked by way of inspection that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements.<br><br>Checked by way of inspection that the procedures are up to date.<br><br>Inspected that data processor has an overview of processing activities and that documentation exists that data processing takes place in accordance with the data processing agreement. | Our tests have not resulted in any material deviations. |
| 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. | Checked by way of inspection that the data processor has a list of processing activities stating localities, countries or regions.<br><br>Inspected one data processing sessions 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. | Our tests have not resulted in any material deviations. |

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

## Use of sub-data processors (control objective F)

| Control objective: Procedures and controls are complied with to ensure that only approved sub-data 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.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's test*** |
| F.1 | Written procedures exist which include requirements for the data processor when using sub-data processors, including requirements for sub-data processing agreements and instructions. | Checked by way of inspection that formalised procedures are in place for using sub-data processors, including requirements for sub-data processing agreements and instructions. | Our tests have not resulted in any material deviations. |
| | Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | Checked by way of inspection that procedures are up to date. | |
| F.2 | The data processor only uses sub-data 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 overview of sub-data processors used. | Our tests have not resulted in any material deviations. |
| | | Checked by way of inspection of a sample of four sub-data processors from the data processor's list of sub-data processors that documentation exists that the processing of data by the sub-data processor is stated in the data processing agreements – or otherwise as approved by the data controller. | |

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

## Use of sub-data processors (control objective F)

| Control objective: Procedures and controls are complied with to ensure that only approved sub-data 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.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's test*** |
| F.3 | When changing the generally approved sub-data 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.<br><br>When changing the specially approved sub-data processors used, this has been approved by the data controller. | Checked by way of inspection that formalised procedures are in place for informing the data controller when changing the sub-data processors used.<br><br>Inspected documentation that the data controller was informed when changing the sub-data processors used throughout the assurance period. | Our tests have not resulted in any material deviations. |
| F.4 | The data processor has subjected the sub-data processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller. | Checked by way of inspection for existence of signed sub-data processing agreements with sub-data processors used, which are stated on the data processor's list.<br><br>Inspected a sample of sub-data processing agreements and contracts that they include the same requirements and obligations as are stipulated in the data processing agreements between the data controllers and the data processor. | Our tests have not resulted in any material deviations. |

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

## Use of sub-data processors (control objective F) - continued

| Control objective: | | | |
|---|---|---|---|
| **Procedures and controls are complied with to ensure that only approved sub-data 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.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's test*** |
| F.5 | The data processor has a list of approved sub-data processors disclosing:<br>• Name;<br>• Business Registration No.;<br>• Address;<br>• Description of the processing. | Checked by way of inspection that the data processor has a complete and updated list of sub-data processors used and approved.<br>Checked by way of inspection that, as a minimum, the list includes the required details about each sub-data processor. | Our tests have not resulted in any material deviations. |

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

## Use of sub-data processors (control objective F) - continued

| Control objective: Procedures and controls are complied with to ensure that only approved sub-data 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.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's test*** |
| F.6 | Based on an updated risk assessment of each sub-data 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-data processor. | Checked by way of inspection that formalised procedures are in place for following up on processing activities at sub-data processors and compliance with the sub-data processing agreements.<br><br>Checked by way of inspection of documentation that each sub-data processor and the current processing activity at such processor are subject-ed to risk assessment.<br><br>Checked by way of inspection of documentation that technical and organisational measures, security of processing at the sub-data processors used, third countries' bases of transfer and similar matters are appropriately followed up on.<br><br>Checked by way of inspection of documentation that information on the follow-up at sub-data processors is communicated to the data controller so that such controller may plan an inspection. | Some sub-data processors have statements that do not cover the full audit period. Where this is the case the data processer has received Bridge Letters covering the relevant periods to cover the full year.<br><br>Our tests have not resulted in any material deviations. |

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

## Transfer to third countries or international organisations (control objective G)

| **Control objective:** **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.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's 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. | Checked by way of inspection 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.<br><br>Checked by way of inspection that procedures are up to date. | Our tests have not resulted in any material deviations. |

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

## Handing out, correcting, deleting or restricting personal data (control objective H)

| **Control objective:**<br>**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.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's 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. | Checked by way of inspection 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>Checked by way of inspection that procedures are up to date. | Our tests have not resulted in any material deviations. |
| H.2 | The data processor has established procedures in so 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. | Checked by way of inspection of documentation that the systems and databases used support the performance of the relevant detailed procedures. | We have been informed that there has not been any requests from data subjects during the audit period.<br><br>Our tests have not resulted in any material deviations. |

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

## Responding to data breaches (control objective I)

| **Control objective:**<br>**Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.** | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's 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. | Checked by way of inspection 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>Checked by way of inspection that procedures are up to date. | Our tests have not resulted in any material deviations. |
| I.2 | The data processor has established the following controls to identify any personal data breaches:<br><br>• Awareness of employees;<br>• Monitoring of network traffic;<br>• Follow-up on logging of access to personal data;<br>• Agreement with third party for assistance on handling security incidents. | Checked by way of inspection that the data processor provides awareness training to the employees in identifying any personal data breaches.<br><br>Checked by way of inspection of documentation that network traffic is monitored and that anomalies, monitoring alarms, large file transfers, etc. are followed up on.<br><br>Checked by way of inspection of documentation that logging of access to personal data, including follow-up on repeated attempts to gain access, is followed up on a timely basis.<br><br>Inspected agreement with third party supplier on possible assistance in handling security incidents. | Our tests have not resulted in any material deviations. |

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

## Responding to data breaches (control objective I) - continued

| Control objective: Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into. | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's test*** |
| I.3 | If any personal data breach occurred, the data processor informed the data controller without undue delay and no later than 24 hours after having become aware of such personal data breach at the data processor or a sub-data processor. | Checked by way of inspection that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach.<br><br>Made inquiries of the sub-data processors as to whether they have identified any personal data breaches throughout the assurance period.<br><br>Checked by way of inspection that the data processor has included any personal data breaches at sub-data processors in the data processor's list of security incidents.<br><br>Inspected a sample of security incidents recorded at the data processor or the sub-data processors have that is has been communicated to the data controllers concerned without undue delay and no later than 24 hours after the data processor became aware of the security incidents. | Our tests have not resulted in any material deviations. |

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

## Responding to data breaches (control objective I) - continued

| Control objective: Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into. | | | |
|---|---|---|---|
| ***Nr.*** | ***Data processor's control activity*** | ***Test performed by auditor*** | ***Result of auditor's 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. | Checked by way of inspection 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>Checked by way of inspection of documentation that the procedures available support that measures are taken to respond to the personal data breach. | We have been informed that there has not been any breaches of personal data during the audit period.<br>Our tests have not resulted in any material deviations. |

PENNEO

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

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

**Jakob Høholdt**
**Underskriver 1**
*Serienummer: PID:9208-2002-2-086945606573*
*IP: 176.22.xxx.xxx*
*2021-01-22 14:09:32Z*
NEM ID

**Anders Grønning Kjærgaard**
**Underskriver 2**
*Serienummer: PID:9208-2002-2-822661869402*
*IP: 212.237.xxx.xxx*
*2021-01-22 14:13:29Z*
NEM ID

**Jacob Helly Juell-Hansen**
**Underskriver 3**
*Serienummer: CVR:34209936-RID:50904197*
*IP: 83.92.xxx.xxx*
*2021-01-22 14:26:09Z*
NEM ID