Assurance report

Sentia Denmark A/S

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with customers throughout the period from 1 January 2024 to 31 December 2024

January 2025

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

Grant Thornton

Table of Contents

Section 1: Sentia Denmark A/S' statement

The accompanying description has been prepared for data controllers, who has signed a data processing agreement with Sentia Denmark 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.

Sentia Denmark A/S uses sub-suppliers and sub-processors. This statement does not include control objectives and related controls at Sentia Denmark A/S' sub-suppliers and 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 Sentia Denmark A/S' description in Section 3 of OSE (Operating System Environment) operated private and public cloud platforms, as well as for co-location, offered by Sentia, can only be achieved if the complementary user entity controls with the data controllers are suitably designed and operationally effective with Sentia Denmark A/S' controls. This assurance report does not include the appropriateness of the design and operational effectiveness of these complementary user entity controls.

Sentia Denmark A/S confirms that:

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

   (i) Presents how Sentia Denmark 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 Sentia Denmark 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 OSE (Operating System Environment) operated private and public cloud platforms, as well as for co-location, offered by Sentia in the processing of personal data in the period from 1 January 2024 to 31 December 2024;

(iii) Does not omit or distort information relevant to the scope of OSE (Operating System Environment) operated private and public cloud platforms, as well as for co-location, offered by Sentia 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 OSE (Operating System Environment) operated private and public cloud platforms, as well as for co-location, offered by Sentia that the individual data controllers might consider important in their particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were, in our view, suitably designed and operated effectively throughout the period from 1 January 2024 to 31 December 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 January 2024 to 31 December 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.

Herlev, 21 January 2025
Sentia Denmark A/S

Mads Jakobsen
CEO

Section 2: Independent auditor's ISAE 3000 assurance report with reasonable assurance on information security and measures pursuant to Sentia Denmark A/S' data processing agreements with data controllers during the period 1 January 2024 to 31 December 2024

To: Sentia Denmark A/S and their customers

Scope

We were engaged to provide assurance about a) Sentia Denmark A/S' description, Section 3 of OSE (Operating System Environment) operated private and public cloud platforms, as well as for co-location, offered by Sentia in accordance with the data processing agreement with data controllers throughout the period from 1 January 2024 to 31 December 2024 and about b+c) the design and operational effectiveness of controls related to the control objectives stated in the Description.

Sentia Denmark A/S uses sub-suppliers and sub-processors. This statement does not include control objectives and related controls with sub-suppliers and sub-processors. Customers who have used Sentia Denmark A/S' services should refer to their specific data processing agreement for detailed information.

Some of the control objectives stated in Sentia Denmark A/S' description in Section 3 of OSE (Operating System Environment) operated private and public cloud platforms, as well as for co-location, offered by Sentia, 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 Sentia Denmark 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.

Sentia Denmark A/S' responsibilities

Sentia Denmark 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 Sentia Denmark 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

OSE (Operating System Environment) operated private and public cloud platforms, as well as for co-location, offered by Sentia 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

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 OSE (Operating System Environment) operated private and public cloud platforms, as well as for co-location, offered by Sentia 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 OSE (Operating System Environment) operated private and public cloud platforms, as well as for co-location, offered by Sentia as designed and implemented throughout the period from 1 January 2024 to 31 December 2024;

(b) The controls related to the control objectives stated in the Description were appropriately designed throughout the period from 1 January 2024 to 31 December 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 January 2024 to 31 December 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 Sentia Denmark A/S' OSE (Operating System Environment) operated private and public cloud platforms, as well as for co-location, offered by Sentia 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, 21 January 2025

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Andreas Moos
Director, CISA, CISM

Section 3: Sentia Denmark A/S' description of processing activity for the supply of OSE (Operating System Environment) operated private and public cloud platforms, as well as for co-location offered by Sentia

The purpose of this description is to provide information for Sentia Denmark A/S' customers and their stakeholders (including auditors) of compliance with the contents of EU's General Data Protection Regulation ("GDPR").

Further, the purpose of this description, is to provide information of the processing security, technical and organisational measures, and responsibilities between the data controller (our customers) and Sentia Denmark A/S.

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 sub-data 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 (Article 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.

G. Transfer to third countries (Article 44)

Sentia transfers only personal data to third party countries if the data controller instructs Sentia to do so. 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.

1.2 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

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

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

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

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

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

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

Method	General description
Inquiries	Interview with appropriate personnel at Sentia Denmark 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

Control activity	GDPR articles	ISO 27701	ISO 27001/2:2013
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.	*Sentia Denmark A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
A.1	Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist to ensure that personal data are only processed according to instructions. We have inspected that the procedures include a requirement to assess at least once a year the need for updates, including in case of changes in the data controller's instructions or changes in the data processing. We have inspected that procedures are up to date.	No deviations noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	We have inspected that management ensures that personal data are only processed according to instructions. We have inspected that a sample of personal data processing operations are conducted consistently with instructions.	No deviations noted.
A.3	The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions.	We have inspected that formalised procedures exist ensuring verification that personal data are not processed against the Regulation or other legislation. We have inspected that procedures are up to date. We have inspected that procedures are in place for informing the data controller of cases where the processing of personal data is evaluated to be against legislation. We have 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. 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.	*Sentia Denmark A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
B.1	Written procedures exist which include a requirement that safeguards agreed are established for the processing of personal data in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist to ensure establishment of the safeguards agreed. We have inspected that procedures are up to date. 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. We have inspected that the risk assessment performed is up to date and comprises the current processing of personal data. We have inspected that the data processor has implemented the technical measures ensuring an appropriate level of security, consistent with the risk assessment. We have inspected that the data processor has implemented the safeguards agreed with the data controller.	No deviations noted.
B.3	For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.	We have inspected that, for the systems and databases used in the processing of personal data, antivirus software has been installed. We have inspected that antivirus software is up to date.	No deviations noted.
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	We have inspected that external access to systems and databases used in the processing of personal data takes place only through a secured firewall. We have inspected that the firewall has been configured in accordance with the relevant internal policy.	No deviations noted.

Control objective B - Technical measures

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

No.	*Sentia Denmark A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	We have inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. We have inspected network diagrams and other network documentation to ensure appropriate segmentation.	No deviations noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	We have inspected that formalised procedures are in place for restricting users' access to personal data. We have inspected that formalised procedures are in place for following up on users' access to personal data being consistent with their work-related need. We have inspected that the technical measures agreed support retaining the restriction in users' work-related access to personal data We have, by sample test, 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. This monitoring comprises: • Availability • Capacity • Incidents	We have inspected that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. We have inspected that a sample of alarms were followed up on and that the data controllers were informed thereof as appropriate.	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.	*Sentia Denmark A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	We have inspected that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. 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.9	Logging of the following matters has been established in systems, databases, and networks:
	
	• Activities performed by system administrators and others holding special rights
	• Security incidents comprising:
	  ○ Changes in log setups, including disabling of logging.
	  ○ Changes in users' system rights
	  ○ Failed attempts to log on to systems, databases, or networks;
	
	Logon data are protected against manipulation and technical errors and are reviewed regularly.
		We have inspected that formalised procedures exist for setting up logging of user activities in systems, databases or networks that are used to process and transmit personal data, including review of and follow-up on logs.
		
		We have inspected that logging of user activities in systems, databases or networks that are used to process or transmit personal data has been configured and activated.
		
		We have inspected that user activity data collected in logs are protected against manipulation or deletion.
		
		We have, by sample test, inspected that the content of a sample of log files is as expected compared to the setup and that documentation exists regarding the follow-up performed and the response to any security incidents.
		
		We have, 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.

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.	*Sentia Denmark A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	We have inspected that formalised procedures exist for regularly testing technical measures, including performing of vulnerability scans and penetration tests. We have, by sample test, inspected that documentation exists regarding regular testing of the technical measures established. We have inspected that any deviations or weaknesses in the technical measures have been responded to in a timely and satisfactory manner and communicated to the data controllers as appropriate.	No deviations noted.
B.12	Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches.	We have inspected that formalised procedures exist for handling changes to systems, databases, or networks, including handling of relevant updates, patches, and security patches. We have inspected extracts from technical security parameters and setups that systems, databases, or networks have been updated using agreed changes and relevant updates, patches, and security patches.	No deviations noted.
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	We have inspected that formalised procedures exist for granting and removing users' access to systems and databases used to process personal data. We have, by sample test, inspected that user accesses granted have been authorised and that a work-related need exists for employees' access to systems and databases. We have, by sample test, inspected resigned or dismissed employees to establish whether their access to systems and databases was deactivated or removed on a timely basis. We have inspected that documentation exists, that user accesses granted are evaluated and authorised on a regular basis – and at least once a year.	No deviations noted.

Control objective B - Technical measures

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

No.	*Sentia Denmark A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
B.14	Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication.	We have inspected that formalised procedures exist to ensure that two-factor authentication is applied in the processing of personal data that involves a high risk for the data subjects. We have inspected that users' access to processing personal data that involve a high risk for the data subjects may only take place by using two-factor authentication.	No deviations noted.
B.15	Physical access safeguards have been established so as to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed.	We have inspected that formalised procedures exist to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed. We have inspected documentation that only authorised persons have had physical access to premises and data centres where 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.	*Sentia Denmark A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
C.1	Management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The IT security policy is based on the risk assessment performed. Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.	We have inspected that an information security policy exists that Management has considered and approved within the past year. We have inspected documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No deviations noted.
C.2	Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.	We have inspected documentation of Management's assessment that the information security policy generally meets the requirements for safeguards and the security of processing in the data processing agreements entered into. We have, by sample test, inspected that the requirements in data processing agreements are covered by the requirements of the information security policy for safeguards and security of processing.	No deviations noted.
C.3	The employees of the data processor are screened as part of the employment process, including: • Test conducted and feedback obtained. • Reference checks performed. • CV obtained • Criminal record obtained.	We have inspected that formalised procedures are in place to ensure screening of the data processor's employees as part of the employment process. We have, by sample test, inspected that the requirements in data processing agreements for screening employees are covered by the data processor's screening procedures. We have, by sample test, inspected that there is documentation that the testing of new employees includes: • Test conducted and feedback obtained. • Reference checks performed. • CV obtained • Criminal record obtained	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.	*Sentia Denmark A/S' control activity*	*Test performed by Grant Thornton*	*Result of 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.	We have inspected that employees appointed have signed a confidentiality agreement. We have inspected that employees ap-pointed have been introduced to: • Information security policy • Procedures for processing data and other relevant information.	No deviations noted.
C.5	For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned.	We have inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal and that assets such as access cards, computers, mobile phones, etc. are returned. We have, 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.	No deviations noted.
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	We have inspected that formalised procedures exist to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality. We have, 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.	No deviations noted.
C.7	Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data.	We have inspected that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data. We have inspected documentation that all employees who have either access to or process personal data have completed the awareness training provided.	No deviations noted.

Control objective D - Return and deletion of personal data

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

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

Control objective E – Storage of personal data

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

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

Control objective F – Use of sub-processors

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

No.	*Sentia Denmark A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
F.1	Written procedures exist which include requirements for the data processor when using sub-processors, including requirements for sub-data processing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place for using sub-data processors, including requirements for sub-data processing agreements and instructions. We have inspected that procedures are up to date.	No deviations noted.
F.2	The data processor only uses sub-processors to process personal data that have been specifically or generally approved by the data controller.	We have inspected that the data processor has a complete and updated list of sub-data processors used. We have, by sample test, inspected 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.	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-data processors used. We have inquired about whether there have been changes to sub-data processors during the period.	We have been informed that there have been no changes in the use of sub-processors during the period. No deviations noted.
F.4	The data processor has subjected the sub-processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	We have inspected the existence of signed sub-data processing agreements with sub-data processors used, which are stated on the data processor's list. 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.	*Sentia Denmark 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-data processors used and approved. We have inspected that, as a minimum, the list includes the required details about each sub-data 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-data processors and compliance with the sub-data processing agreements. We have inspected documentation that each sub-data processor and the current processing activity at such processor are subjected to risk assessment. We have inspected documentation that technical and organisational measures, security of processing at the sub-data processors used, third countries' bases of transfer and similar matters are appropriately followed up on. We have inspected 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.	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.	*Sentia Denmark A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
G.1	Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist to ensure that personal data are only transferred to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. We have inspected that procedures are up to date.	No deviations noted.
G.2	The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.	We have inquired whether the data processor has transferred personal data to third countries or international organisations	We have been informed that personal data has not been transferred to third countries or international organisations. No deviations noted.
G.3	As part of the transfer of personal data to third countries or international organisations, the data processor assessed and documented the existence of a valid basis of transfer.	We have inquired whether the data processor has transferred personal data to third countries or international organizations during the declaration period.	We have been informed that personal data has not been transferred to third countries or international organisations. No deviations noted.

Control objective H – Rights of the data subjects

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

No.	*Sentia Denmark A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
H.1	Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects. We have inspected that procedures are up to date.	No deviations noted.
H.2	The data processor has established procedures as far as this was agreed that enable timely assistance to the data controller in handing out, correcting, deleting, or restricting or providing information about the processing of personal data to data subjects.	We have inspected that the procedures in place for assisting the data controller, include detailed procedures for: • Handing out data • Correcting data • Deleting data • Restricting the processing of personal data • Providing information about the processing of personal data to data subjects. We have inquired whether the data processor has received requests from the data controller in relation to the rights of the data subjects We have 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. 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.	*Sentia Denmark A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
I.1	Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. We have inspected that procedures are up to date.	No deviations noted.
I.2	The data processor has established the following controls to identify any personal data breaches: • Awareness of employees • Monitoring of network traffic • Follow-up on logging of access to personal data.	We have inspected that the data processor provides awareness training to the employees in identifying any personal data breaches. We have inspected documentation that network traffic is monitored and that anomalies, monitoring alarms, large file transfers, etc. are followed up on. We have inspected documentation that logging of access to personal data, including follow-up on repeated attempts to gain access, is followed up on, on a timely basis.	No deviations noted.
I.3	If any personal data breach occurred, the data processor informed the data controller without undue delay after having become aware of such personal data breach at the data processor or a sub-processor.	We have inspected that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach. We have inspected that the data processor has included any personal data breaches at sub-data processors in the data processor's list of security incidents. We have inspected that all personal data breaches recorded at the data processor or the sub-data processors have been communicated to the data controllers concerned, without undue delay, after the data processor became aware of the personal data breach.	No deviations noted.

Control objective I – Managing personal data breaches

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

No.	*Sentia Denmark A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency: • Nature of the personal data breach • Probable consequences of the personal data breach • Measures taken or proposed to be taken to respond to the personal data breach.	We have inspected that the procedures in place for informing the data controllers in the event of any personal data breach include detailed procedures for: We have inspected documentation that, when a personal data breach occurred, measures were taken to respond to such breach.	No deviations noted.