

Assurance report

Lessor Group

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with customers using Lessor Group's SaaS solutions within payroll and HR administration, shop floor management, time recording and workforce management throughout the period from 1 April 2023 to 31 March 2024

July 2024

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

Table of Contents

Section 1:	Lessor Group's statement	1
Section 2:	Independent auditor's ISAE 3000 assurance report with reasonable assurance on information security and measures pursuant to Lessor Group's data processing agreements with customers throughout the period 1 April 2023 to 31 March 2024	3
Section 3:	Lessor Group's description of processing activity for the provision and operation of SaaS solutions within payroll and HR administration, shop floor management, time recording and workforce management.....	5
Section 4:	Control objectives, controls, tests, and results hereof.....	8

Section 1: Lessor Group's statement

The purpose of this description is to provide information for Lessor Group's entities (Lessor A/S, Danske Lønssystemer A/S and Emply International ApS) customers and their stakeholders. Throughout this document, the term Lessor Group refers to these companies.

The description has been prepared for data controllers, who has signed a data processing agreement with Lessor Group, 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.

Lessor Group uses the following sub-processors: Netic A/S, NetNordic Denmark A/S, PostNord Strålfors A/S, Post Danmark A/S, Contractbook ApS, Bogholdergruppen.DK ApS, Compaya A/S, Trifork Security A/S and Interlogic Danmark ApS. This statement does not include control objectives and related controls at Lessor Group's sub-processors. Certain control objectives in the description can only be achieved, if the sub-processor's controls, assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities performed by sub-processors.

Some of the control areas, stated in Lessor Group's description in Section 3 of provision and operation of SaaS solutions within payroll and HR administration, shop floor management, time recording and workforce management, can only be achieved if the complementary user entity controls with the data controllers are suitably designed and operationally effective with Lessor Group's controls. This assurance report does not include the appropriateness of the design and operational effectiveness of these complementary user entity controls.

Lessor Group confirms that:

- a) The accompanying description, Section 3, fairly presents how Lessor Group has processed personal data for data controllers subject to the Regulation throughout the period from 1 April 2023 to 31 March 2024. The criteria used in making this statement were that the accompanying description:
 - (i) Presents how Lessor Group'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 provision and operation of SaaS solutions within payroll and HR administration, 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 provision and operation of SaaS solutions within payroll and HR administration, shop floor management, time recording and workforce management in the processing of personal data in the period from 1 April 2023 to 31 March 2024;
 - (iii) Does not omit or distort information relevant to the scope of provision and operation of SaaS solutions within payroll and HR administration, shop floor management, time recording and workforce management 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 provision and operation of SaaS solutions within payroll and HR administration, shop floor management, time recording and workforce management that the individual data controllers might consider important in their particular circumstances.
- b) The controls related to the control objectives stated in the accompanying description were, in our view, suitably designed and operated effectively throughout the period from 1 April 2023 to 31 March 2024 if relevant controls with sub-processors were operationally effective and data controller has performed the complementary user entity controls, assumed in the design of Lessor Group's controls as of 1 April 2023 to 31 March 2024. The criteria used in making this statement were that:
- (i) The risks that threatened achievement of the control objectives stated in the description were identified
 - (ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and
 - (iii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 April 2023 to 31 March 2024.
- c) Appropriate technical and organisational safeguards were established and maintained to comply with the agreements with the data controllers, sound data processing practices and relevant requirements for data processors in accordance with the Regulation.

Allerød, 3 July 2024

Lessor Group ApS

on behalf of Lessor A/S, Danske Lønssystemer A/S and Emply International ApS

Henrik Møller

Chief Executive Officer

Section 2: Independent auditor's ISAE 3000 assurance report with reasonable assurance on information security and measures pursuant to Lessor Group's data processing agreements with customers throughout the period 1 April 2023 to 31 March 2024

To: Lessor Group (Empty International ApS, Danske Lønssystemer A/S and Lessor A/S) and their customers

Scope

We were engaged to provide assurance about a) Lessor Groups' description, Section 3 of provision and operation of SaaS solutions within payroll and HR administration, shop floor management, time recording and workforce management in accordance with the data processing agreement with customers throughout the period from 1 April 2023 to 31 March 2024 and about b+c) the design and operational effectiveness of controls related to the control objectives stated in the description. Lessor Group uses the following sub-processors, Netic A/S, NetNordic Denmark A/S, PostNord Strålfors A/S, Post Danmark A/S, Contractbook ApS, Bogholdergruppen.DK ApS, Compaya A/S, Trifork Security A/S and Interlogic Danmark ApS. This statement does not include control objectives and related controls at Lessor Group's sub-processors. Certain control objectives in the description can only be achieved if the sub-processor's controls, assumed in the design of our controls, are appropriately designed, and operating effectively. The description does not include control activities performed by sub-processor. Some of the control objectives stated in Lessor Group's description in Section 3 of provision and operation of SaaS solutions within payroll and HR administration, shop floor management, time recording and workforce management, 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 Lessor Group. The report does not include the appropriateness of the design and operational effectiveness of these complementary user entity controls.

Lessor Group's responsibilities

Lessor Group 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 Lessor Group'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 provision and operation of SaaS solutions within payroll and HR administration, shop floor management, time

recording and workforce management 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

Lessor Group's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of provision and operation of SaaS solutions within payroll and HR administration, shop floor management, time recording and workforce management 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 in Section 1. In our opinion, in all material respects:

- (a) The description fairly presents provision and operation of SaaS solutions within payroll and HR administration, shop floor management, time recording and workforce management as designed and implemented throughout the period from 1 April 2023 to 31 March 2024;
- (b) The controls related to the control objectives stated in the description were appropriately designed throughout the period from 1 April 2023 to 31 March 2024; to obtain reasonable assurance that the control objectives stated in the description would be obtained if controls with sub-processor were operating effectively and if data controller has designed and implemented the complementary user entity controls, assumed in the design of Lessor Group's controls throughout the period from 1 April 2023 to 31 March 2024, and
- (c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 April 2023 to 31 March 2024.

Description of tests of controls

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

Intended users and purpose

This report and the description of tests of controls in Section 4 are intended only for data controllers who have used Lessor Group's provision and operation of SaaS solutions within payroll and HR administration, shop floor management, time recording and workforce management 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, 3 July 2024

Grant Thornton

Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Andreas Moos
Director, CISA, CISM

Section 3: Lessor Group's description of processing activity for the provision and operation of SaaS solutions within payroll and HR administration, shop floor management, time recording and workforce management

The purpose of this description is to provide information for Lessor Group's entities' (Lessor A/S, Danske Lønssystemer A/S and Emply International ApS) customers and their stakeholders (including auditors) regarding the requirements and contents of the EU General Data Protection Regulation ("GDPR"). Throughout this document, the term Lessor Group refers to these companies.

Additionally, the purpose of this description is to provide specific information on matters regarding the security of processing, technical and organisational measures, responsibility between data controllers (our customers) and processor (Lessor Group), and how the services offered can help support the data subjects' rights.

Lessor Group

Lessor Group offers a wide range of solutions within payroll and HR administration, shop floor management, time recording and workforce management.

Risk management in Lessor Group

Lessor Group have produced Data Protection Impact Assessments for all our services.

Organisation and responsibility

Lessor Group has a clear and transparent corporate structure and employs over 450 employees.

The organisational structure of the Lessor Group includes the departments Administration, Finance, Development, Support, IT-security and IT Operations as well as various product departments.

The employees of the Lessor Group are thus responsible for the support of our own products as well as the hosting infrastructure. The support teams handle all incoming questions. They either solve the problems or pass on the task to the Operations Department for further processing.

Thus, the Operations Department acts as second line support and monitors existing operating solutions and other tasks associated with the day-to-day management of our hosting environment.

GDPR and Lessor Group's role and responsibility as a processor

We refer to our Data Protection Impact Assessment documents.

Processing of various categories of personal data

We process all personal data as confidential.

Rights of the data subject

For all services, we have prepared a procedure / description of how the data processor meets the data subject's rights. These may be obtained from our support, or our support can assist in solving the task.

General obligations as processor

All sub-processors are listed in our data processing agreements as well as on our websites. We audit our sub-processors annually.

Data protection officer (DPO)

Lessor Group has DPO-Danmark as external DPO.

Transfer of personal data

We do not store personal/customer data outside the EU/EEA.

Security of processing, notification, and communication

We have defined our quality standards system based on the general objective of providing our customers with a stable and secure hosting solution. To comply with the objectives, we have implemented policies and procedures which ensure that our supplies are uniform and transparent.

Our IT security policy is produced in accordance with ISO 27001:2022 and applies to all employees and all deliveries.

Our methodology for the implementation of controls is defined with reference to ISO 27002:2022 (guidelines for information security management) and is thus divided into the following control areas:

- Information security policies
- Organisation of information security
- Employee safety
- Asset management
- Conditional access
- Cryptography
- Physical security and environmental safeguards
- Operational safety
- Communication security
- Purchase, development, and maintenance of systems
- Supplier relationships
- Information security breach management
- Information security aspects related to emergency and restoration management
- Compliance

Privacy by design/default

We have prepared a procedure to ensure privacy by design.

Deletion policy

We have a deletion policy and we have quarterly "deletion days" where we assure that any unstructured data (e.g., e-mails, papers etc.) that we no longer have a work-related need to keep, are deleted / shredded.

Compliance

Our Legal and Compliance team keeps itself updated via newsgroups, workshops etc. to ensure that Lessor Group and the services we offer, comply with the current GDPR legislation.

Complementary controls of data controllers

The data controller has the following obligations:

- ensuring that personal data is up to date
- ensuring that the instruction is lawful in relation to the personal data law regulation in force at any given time
- that the instruction is appropriate in relation to this data processing agreement and the main service
- ensuring that the data controller's users are up to date
- ensuring that no personal data is handed over to 3rd party unless it is to fulfil legislation

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-J below. Our test has included the controls, we find necessary to establish reasonable assurance for compliance with the articles stated throughout the period from 1 April 2023 to 31 March 2024.

Our statement, does not apply to controls, performed at Lessor Group' sub-processors.

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

We performed our test of controls at Lessor Group by the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at Lessor Group. 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	<i>New scope compared to ISO 27001/2</i>
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	<i>New scope compared to ISO 27001/2</i>
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	<i>New scope compared to ISO 27001/2</i>
D.1	6, 11, 13, 14, 32	7.4.5, 7.4.7, 7.4.4	<i>New scope compared to ISO 27001/2</i>
D.2	6, 11, 13, 14, 32	7.4.5, 7.4.7, 7.4.4	<i>New scope compared to ISO 27001/2</i>
D.3	13, 14	7.4.7, 7.4.4	<i>New scope compared to ISO 27001/2</i>
E.1	13, 14, 28, 30	8.4.2, 7.4.7, 7.4.8	<i>New scope compared to ISO 27001/2</i>
E.2	13, 14, 28, 30	8.4.2, 7.4.7, 7.4.8	<i>New scope compared to ISO 27001/2</i>
F.1	6, 8, 9, 10, 17, 18, 22, 24, 25, 28, 32, 35, 40, 41, 42	5.2.1, 7.2.2, 7.2.6, 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7	15
F.2	28	8.5.7	15
F.3	28	8.5.8, 8.5.7	15
F.4	33, 34	6.12.1.2	15
F.5	28	8.5.7	15
F.6	33, 34	6.12.2	15.2.1-2
G.1	15, 30, 44, 45, 46, 47, 48, 49	6.10.2.1, 7.5.1, 7.5.2, 7.5.3, 7.5.4, 8.5.1, 8.5.2, 8.5.3	13.2.1, 13.2.2
G.2	15, 30, 44, 45, 46, 47, 48, 49	6.10.2.1, 7.5.1, 7.5.2, 7.5.3, 7.5.4, 8.4.2, 8.5.2, 8.5.3	13.2.1
G.3	15, 30, 44, 45, 46, 47, 48, 49	6.10.2.1, 7.5.1, 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
H.1	12, 13, 14, 15, 20, 21	7.3.5, 7.3.8, 7.3.9	<i>New scope compared to ISO 27001/2</i>
H.2	12, 13, 14, 15, 20, 21	7.3.5, 7.3.8, 7.3.9	<i>New scope compared to ISO 27001/2</i>
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.	Lessor Group'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.	<p>We have inspected that formalised procedures exist to ensure that personal data are only processed according to instructions.</p> <p>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.</p> <p>We have inspected that procedures are up to date.</p>	No deviations noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	<p>We have inspected that management ensures that personal data are only processed according to instructions.</p> <p>We have inspected that a sample of personal data processing operations are conducted consistently with instructions.</p>	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.	<p>We have inspected that formalised procedures exist ensuring verification that personal data are not processed against the Regulation or other legislation.</p> <p>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 in violation of the legislation.</p> <p>We have inquired about if the data processor has received instructions that are against the GDPR or other data protection legislation.</p>	<p>We have been informed that the data processor has not received any instructions that infringes the GDPR or other data protection legislation.</p> <p>No deviations noted.</p>

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.	Lessor Group's control activity	Test performed by Grant Thornton	Result of test
B.1	<p>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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have inspected that formalised procedures exist to ensure establishment of the safeguards agreed.</p> <p>We have inspected that procedures are up to date.</p> <p>We have, by sample test, inspected that the safeguards agreed in the data processing agreements, have been established.</p>	No deviations noted.
B.2	<p>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.</p>	<p>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.</p> <p>We have inspected that the risk assessment performed is up to date and comprises the current processing of personal data.</p> <p>We have inspected that the data processor has implemented the technical measures ensuring an appropriate level of security consistent with the risk assessment.</p> <p>We have inspected that the data processor has implemented the safeguards agreed with the data controller.</p>	No deviations noted.
B.3	<p>For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.</p>	<p>We have inspected that, for the systems and databases used in the processing of personal data, antivirus software has been installed.</p> <p>We have inspected that antivirus software is up to date.</p>	No deviations noted.
B.4	<p>External access to systems and databases used in the processing of personal data takes place through a secured firewall.</p>	<p>We have inspected that external access to systems and databases used in the processing of personal data takes place only through a secured firewall.</p> <p>We have inspected that the firewall has been active and updated.</p>	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.	Lessor Group'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.	<p>We have inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.</p> <p>We have inspected network diagrams and other network documentation to ensure appropriate segmentation.</p>	No deviations noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	<p>We have inspected that formalised procedures are in place for restricting users' access to personal data.</p> <p>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.</p> <p>We have inspected that the technical measures agreed support retaining the restriction in users' work-related access to personal data.</p> <p>We have inspected that access is restricted to the employees' work-related need for a sample of users' access to systems and databases.</p>	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.	<p>We have inspected that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.</p> <p>We have inspected that a sample of alarms were followed up on and that the data controllers were informed thereof as appropriate.</p>	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.	Lessor Group's control activity	Test performed by Grant Thornton	Result of test
B.8	<p>Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.</p>	<p>We have inspected that formalised procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognised algorithm.</p> <p>We have inspected that technological encryption solutions have been available and active throughout the assurance period.</p> <p>We have inspected that encryption is applied when transmitting confidential and sensitive personal data through the internet.</p>	No deviations noted.
B.9	<p>Logging has been established in systems, databases, and networks.</p> <p>Log data are protected against manipulation, technical errors and are reviewed regularly.</p>	<p>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.</p> <p>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.</p> <p>We have inspected that user activity data collected in logs are protected against manipulation or deletion.</p> <p>We have inspected that the content of a sample of log files is as expected compared to the setup and we have inspected that documentation exists regarding the follow-up performed and the response to any security incidents.</p> <p>We have inspected that documentation exists for the follow-up performed for activities carried by system administrators and others holding special rights.</p>	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.	Lessor Group's control activity	Test performed by Grant Thornton	Result of test
B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.	<p>We have inspected that formalised procedures exist for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised form.</p> <p>We have, by sample test, inspected that personal data included in development or test databases are pseudonymised or anonymised.</p> <p>We have, by sample test, inspected development or test databases in which personal data are not pseudonymised or anonymised that this has taken place according to agreement with, and on behalf of, the data controller.</p>	No deviations noted.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	<p>We have inspected that formalised procedures exist for regularly testing technical measures, including for performing vulnerability scans and penetration tests.</p> <p>We have inspected samples that documentation exists regarding regular testing of the technical measures established.</p> <p>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.</p>	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.	<p>We have inspected that formalised procedures exist for handling changes to systems, databases, or networks, including handling of relevant updates, patches, and security patches.</p> <p>We have, by sample test, inspected that changes and patched to systems and databases are performed according to the procedure for change management and patch management, including approval and tests before implementation.</p>	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.	Lessor Group's control activity	Test performed by Grant Thornton	Result of test
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	<p>We have inspected that formalised procedures exist for granting and removing users' access to systems and databases used to process personal data.</p> <p>We have inspected that documentation exists that user accesses granted are evaluated and authorised on a regular basis – and at least once a year.</p>	No deviations noted.
B.14	Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication.	<p>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.</p> <p>We have inspected that users' access to processing personal data that involve a high risk for the data subjects can only take place by using two-factor authentication.</p>	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.	<p>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.</p> <p>We have inspected documentation that, throughout the assurance period, only authorised persons have had physical access to premises and data centres at which personal data are stored and processed.</p>	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.	Lessor Group's control activity	Test performed by Grant Thornton	Result of test
C.1	<p>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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.</p>	<p>We have inspected that an information security policy exists that management has considered and approved within the past year.</p> <p>We have inspected documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.</p>	No deviations noted.
C.2	<p>Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.</p>	<p>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.</p> <p>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.</p>	No deviations noted.
C.3	<p>The employees of the data processor are screened as part of the employment process.</p>	<p>We have inspected that formalised procedures are in place to ensure screening of the data processor's employees as part of the employment process.</p> <p>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.</p> <p>We have, by sample test, inspected that there is documentation that the testing of new employees during the audit period has included:</p> <ul style="list-style-type: none"> • Criminal record 	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.	Lessor Group'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.	<p>We have, by sample test, inspected that employees appointed during the assurance period have signed a confidentiality agreement.</p> <p>We have, by sample test, inspected that employees appointed during the assurance period have been introduced to:</p> <ul style="list-style-type: none"> • 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.	<p>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.</p> <p>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.</p>	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.	<p>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.</p> <p>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.</p>	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.	Lessor Group's control activity	Test performed by Grant Thornton	Result of test
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.	<p>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.</p> <p>We have inspected documentation that all employees who have either access to or process personal data have completed the awareness training provided.</p>	No deviations noted.
C.8	The processor has assessed the need for a DPO and has ensured that the DPO has the adequate professional competence to perform their tasks and are involved in relevant areas.	We have inspected documentation for the DPO's qualifications, are in accordance with the role description.	No deviations noted.
C.9	<p>The processor keeps a record of categories of processing activities for each data controller.</p> <p>Management has ensured that the record of categories of processing activities for each controller includes:</p> <ul style="list-style-type: none"> Name and contact information of the data processor, the data controller, representatives of the data controller and data protection officers The categories of processing, carried out on behalf of the individual data controller. When relevant, information about transfer to third countries or an international organisation, with documentation of adequate guarantees. Where possible, a general description of technical and organisational security measures. <p>Regularly – and at least annually – an assessment is made of whether the record of categories of processing activities for each controller should be updated.</p>	<p>We have inspected that the category of processing contains the following information:</p> <ul style="list-style-type: none"> the name and contact details of the processor, and the data protection officer the categories of processing carried out on behalf of each controller when relevant, transfers of personal data to a third country or an international organisation where possible, a general description of the technical and organisational security measures. <p>We have inspected that the categories of processing activities have been updated and approved by management during the period.</p>	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.	Lessor Group's control activity	Test performed by Grant Thornton	Result of test
D.1	<p>Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have inspected that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller.</p> <p>We have inspected that the procedures are up to date.</p>	No deviations noted.
D.2	<p>Specific requirements have been agreed with respect to the data processor's storage periods and deletion routines.</p>	<p>We have inspected that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines.</p> <p>We have, by sample test, inspected that documentation exists of personal data being stored in accordance with the storage periods agreed in data processing agreements.</p> <p>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.</p>	No deviations noted.
D.3	<p>Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been:</p> <ul style="list-style-type: none"> Returned to the data controller; and/or Deleted if this is not in conflict with other legislation. 	<p>We have inspected that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data.</p> <p>We have, by sample test, inspected that documentation exists of personal data being stored in accordance with the storage periods agreed in data processing agreements.</p> <p>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.</p>	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.	Lessor Group's control activity	Test performed by Grant Thornton	Result of test
E.1	<p>Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have inspected that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements.</p> <p>We have inspected that the procedures are up to date.</p>	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.	<p>We have inspected that the data processor has a complete and updated list of processing activities stating localities, countries, or regions.</p> <p>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.</p>	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.	Lessor Group's control activity	Test performed by Grant Thornton	Result of test
F.1	<p>Written procedures exist which include requirements for the data processor when using sub-processors, including requirements for sub-data processing agreements and instructions.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have inspected that formalised procedures are in place for using sub-processors, including requirements for sub-data processing agreements and instructions.</p> <p>We have inspected that procedures are up to date.</p>	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.	<p>We have inspected that the data processor has a complete and updated list of sub-processors used.</p> <p>We have, by sample test, inspected that documentation exists that the processing of data by the sub-processor is stated in the data processing agreements – or otherwise as approved by the data controller.</p>	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.	<p>We have inspected that formalised procedures are in place for informing the data controller when changing the sub-processors used.</p> <p>We have inspected documentation that the data controller was informed when changing the sub-processors used throughout the assurance period.</p>	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.	<p>We have inspected the existence of signed sub-data processing agreements with sub-processors used, which are stated on the data processor's list.</p> <p>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.</p>	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.

<i>No.</i>	<i>Lessor Group's control activity</i>	<i>Test performed by Grant Thornton</i>	<i>Result of test</i>
F.5	The data processor has a list of approved sub-processors.	<p>We have inspected that the data processor has a complete and updated list of sub-processors used and approved.</p> <p>We have inspected that, as a minimum, the list includes the required details about each sub-processor.</p>	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.	<p>We have inspected that formalised procedures are in place for following up on processing activities at sub-processors and compliance with the sub-data processing agreements.</p> <p>We have inspected documentation that each sub-processor and the current processing activity at such processor are subjected to risk assessment.</p> <p>We have inspected documentation that technical and organisational measures, security of processing at the sub-processors used, third countries' bases of transfer and similar matters are appropriately followed up on.</p> <p>We have inspected documentation that information on the follow-up at sub-processors is communicated to the data controller so that such controller may plan an inspection.</p>	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.	Lessor Group's control activity	Test performed by Grant Thornton	Result of test
G.1	<p>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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>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.</p> <p>We have inspected that procedures are up to date.</p>	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 into whether the data processor have transferred data to third countries or international organisations.	<p>We have been informed that no personal data have been transferred to third countries or international organisation during the audit period.</p> <p>No deviations noted.</p>
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 into whether the data processor have transferred data to third countries or international organisations.	<p>We have been informed that no personal data have been transferred to third countries or international organisation during the audit period.</p> <p>No deviations noted.</p>

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.	Lessor Group's control activity	Test performed by Grant Thornton	Result of test
H.1	<p>Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>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.</p> <p>We have inspected that procedures are up to date.</p>	No deviations noted.
H.2	<p>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.</p>	<p>We have inspected documentation that the used systems and servers support functionality so that the data controller can handle requests themselves.</p> <p>We have inquired into whether the data processor have received any request in relation to the rights of the data subject during the audit period.</p>	<p>We have been informed that the data processor has not received any request related to the rights of the data subjects during the audit period.</p> <p>No deviations noted.</p>

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.	Lessor Group's control activity	Test performed by Grant Thornton	Result of test
I.1	<p>Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>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.</p> <p>We have inspected that procedures are up to date.</p> <p>We have inspected that the procedure is communicated to employees.</p>	No deviations noted.
I.2	The data processor has established controls for identification of possible personal data breaches.	<p>We have inspected that the data processor provides awareness training to the employees in identifying any personal data breaches.</p> <p>We have inspected documentation that network traffic is monitored and that anomalies, monitoring alarms, large file transfers, etc. are followed up on.</p> <p>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.</p>	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.	<p>We have inspected that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach.</p> <p>We have inquired that the data processor has included any personal data breaches at sub-processors in the data processor's list of security incidents.</p> <p>We have inspected that all personal data breaches recorded at the data processor, or the sub-processors have been communicated to the data controllers concerned without undue delay after the data processor became aware of the personal data breach.</p>	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.

<i>No.</i>	<i>Lessor Group's control activity</i>	<i>Test performed by Grant Thornton</i>	<i>Result of test</i>
I.4	<p>The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency:</p> <ul style="list-style-type: none"> • 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. 	<p>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:</p> <ul style="list-style-type: none"> • Describing the nature of the personal data breach • Describing the probable consequences of the personal data breach • Describing measures taken or proposed to be taken to respond to the personal data breach. <p>We have inspected documentation that, when a personal data breach occurred, measures were taken to respond to such breach.</p>	No deviations noted.