Assurance report

Lessor Group ApS

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 April 2022 to 31 March 2023

July 2023

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 ApS' description of processing activity for the supply of Lessor Group ApS' services

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

The purpose of this description is to supply information to Lessor Group's customers and their stakeholders (including auditors) regarding the requirements and contents of the EU General Data Protection Regulation ("GDPR").

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.

Services in Lessor Group are: Lessor4 Løn, Lessor4 Tid, Lessor App, LessorLøn, LessorLøn SaaS, Payroll to Microsoft Dynamics NAV, Human Resource to Microsoft Dynamics NAV, Time & Attendance to Microsoft Dynamics NAV, Payroll to Microsoft Dynamics AX, LessorPM HR, LessorPM Payroll, LessorPortalen, Lessor SP Tid, Danløn, Danløn App, LessorWorkforce and Lessor Workforce APP.

Lessor Group and our Services

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

We have produced Data Protection Impact Assessments for all our services.

Organisation and responsibility

Lessor Group has a clear and transparent corporate structure and employs approximately 180 employees. The organizational structure of the Lessor Group includes the departments Administration, Finance, Development, Support 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 consider 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 an external DPO.

Transfer of personal data

We do not store data outside the EU/EEA or in third countries.

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 27002:2013 and applies to all employees and all deliveries.

Our methodology for the implementation of controls is defined with reference to ISO 27002:2013 (guidelines for information security management) and is thus divided into the following control areas:

- Information security policies
- Organization 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 be 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.

Changes in the audit period

A new Lessor App has been added.

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 2: Lessor Group ApS' statement

The accompanying description has been prepared for data controllers, who has signed a data processing agreement with Lessor Group ApS, 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 ApS uses the following sub-suppliers and sub-processors, Post Danmark A/S, Compaya A/S, Emply International ApS, NetNordic A/S, and InterLogic Danmark ApS. In addition, Danløn HR uses Contractbook A/S. This statement does not include control objectives and related controls at Lessor Group ApS' sub-suppliers and sub-processors.

Lessor Group ApS confirms that:

a) The accompanying description, Section 1, fairly presents how Lessor Group ApS has processed personal data for data controllers subject to the Regulation throughout the period from 1 April 2022 to 31 March 2023. The criteria used in making this statement were that the accompanying description:

   (i) Presents how Lessor Group ApS' 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 Lessor Group ApS' services 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 Lessor Group ApS' services in the processing of personal data in the period from 1 April 2022 to 31 March 2023;

(iii) Does not omit or distort information relevant to the scope of Lessor Group ApS' services being described for the processing of personal data while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Lessor Group ApS' services that the individual data controllers might consider important in their particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were, in our view, suitably designed and operated effectively throughout the period from 1 April 2022 to 31 March 2023. If relevant controls with sub-suppliers were operationally effective and data controller has performed the complementary controls, assumed in the design of Lessor Group ApS' controls as of 1 April 2022 to 31 March 2023. The criteria used in making this statement were that:

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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 April 2022 to 31 March 2023.

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, 21 July 2023
Lessor Group ApS

Henrik Møller
CEO

Section 3: Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to Lessor Group ApS' data processing agreement with customers

To: Lessor Group ApS and their customers

Scope

We were engaged to provide assurance about a) Lessor Group ApS' description, Section 1, of Lessor Group ApS' services in accordance with the data processing agreement with costumers as data controllers throughout the period from 1 April 2022 to 31 March 2023 and about b) and c) the design and operating effectiveness of controls related to the control objectives stated in the Description.

Lessor Group ApS uses the following sub-suppliers and sub-processors, Post Danmark A/S, Compaya A/S, Emply International ApS, NetNordic A/S, and InterLogic Danmark ApS. In addition, Danløn HR uses Contractbook A/S. This statement does not include control objectives and related controls at Lessor Group ApS' sub-suppliers and sub-processors.

We express reasonable assurance in our conclusion.

Lessor Group ApS' responsibilities

Lessor Group ApS is responsible for: preparing the Description and the accompanying statement, Section 2, including the completeness, accuracy, and the method of presentation of the Description and statement, providing the services covered by the Description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

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 is subject to the International Standard on Quality Control (ISQC 1)[1] and accordingly uses and maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on Lessor Group ApS' Description and on the design and operating effectiveness of controls related to the control objectives stated in that Description, based on our procedures.

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

[1] ISQC 1, Quality control for firms that perform audits and reviews of financial statements, and other assurance and related services engagements.

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 services and about the design and operating effectiveness of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not appropriately designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the Description, the appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data processor and described in Section 2.

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

Basis for qualified opinion

Lessor Group ApS states in Section 1 that procedures and controls exist to ensure that all sub-processors are listed in the data processing agreements. We have however ascertained that Lessor Group ApS has made use of a sub-processor which were not approved by or communicated in a timely manner to new Data Controllers from 20 October 2022 to 31 December 2022.

Qualified opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the *Management's statement* section. In our opinion, with the exception of the area mentioned in "Basis for qualified opinion" that in all material respects:

(a) The Description fairly presents Lessor Group ApS' services as designed and implemented throughout the period from 1 April 2022 to 31 March 2023;

(b) The controls related to the control objectives stated in the Description were appropriately designed throughout the period from 1 April 2022 to 31 March 2023; 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 2022 to 31 March 2023.

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 ApS' services, who have a sufficient understanding to consider it along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the Regulation have been complied with.

Copenhagen, 21 July 2023

Grant Thornton
State Authorised Public Accountants

Kristian Randløv Lydolph
State Authorised Public Accountant

Martin Brogaard Nielsen
Partner, CISA, CIPP/E, CRISC

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

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

Our test of the functionality has included the control objectives and attached controls, selected by management and which are stated in the control objectives A-I below. Our test has included the controls, we find necessary to establish reasonable assurance for compliance with the articles stated throughout the period from 1 April 2022 to 31 March 2023.

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

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

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

Method	General description
Inquiries	Interview with appropriate personnel at Lessor Group ApS. The interviews have included questions about, how controls are performed.
Observation	Observing how controls are performed.
Inspection	Reading of documents and reports, including description of the performance of the control. This includes reading and assessment of reports and documents to evaluate whether the specific controls are designed in such a way, that they can the expected to be effective when implemented.
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
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
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.	*Lessor Group ApS' control activity*	*Grant Thornton's test*	*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, by sample test, inspected that 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 in place for informing the data controller of cases where the processing of personal data is considered to be against legislation. We have inquired if data controllers were informed in cases where the processing of personal data was considered to be against legislation.	We have been informed that there have been no cases where the processing of personal data was considered to be in violation of legislation, why we have not tested the effectiveness of the control. 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 ApS' control activity*	*Grant Thornton's test*	*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 upon in 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.	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.
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	We have inspected the network policy. We have inspected network diagrams and other network documentation to ensure appropriate segmentation.	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 ApS' control activity*	*Grant Thornton's test*	*Result of test*
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 inspected that access is restricted to the employees' work-related need for a sample of users' access to systems and databases.	No deviations noted.
B.7	For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.	We have inspected that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. We have, by sample test, inspected that alarms were followed up on and that the data controllers were informed thereof as appropriate.	No deviations noted.
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	We have inspected that formalised procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognised algorithm. We have inspected that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email. We have inquired about the use of transport layer security.	We have observed that Workforce is supported by TLS 1.0 and TLS 1.1. No further deviations noted.

Control objective B - Technical measures

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

No.	*Lessor Group ApS' control activity*	*Grant Thornton's test*	*Result of test*
B.9	Logging has been established in systems, databases, and networks that support the processing of personal data. Log data are protected against manipulation, 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. 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 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 inspected that documentation exists for the follow-up performed for activities carried by system administrators and others holding special rights.	No deviations noted.
B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.	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. We have, by sample test, inspected that personal data included in development or test databases are pseudonymised or anonymised.	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 ApS' control activity*	*Grant Thornton's test*	*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 the 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.	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, by sample test, inspected whether a selection of changes, made on service applications have been registered, assessed, prioritized, and implemented in the production environment, according to the Change Management procedure. We have inquired about the change management procedure for IT Operations.	We have from 63 samples observed that: • 8 samples were not approved • 2 samples no segregation of duties was present We have been informed that a risk assessment is performed for all changes to systems, databases and networks but that the risk assessment is not formally documented at this moment. No further deviations noted.

Control objective B - Technical measures

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

No.	*Lessor Group ApS' control activity*	*Grant Thornton's test*	*Result of test*
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	We have inspected that formalised procedures exist for granting and removing users' access to systems and databases using to process personal data. We have inspected that the user accesses granted have been authorised and that a work-related need exists for a sample of 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.	We have observed that for 1 out of 13 samples no ticket of approval was available for access creation. We have observed that no formal review of user access rights has been performed for Danløn and LessorLøn. No further deviations noted.
B.14	Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication.	We have inspected that 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, throughout the assurance period, only authorised persons have had physical access to premises and data centres at which personal data are stored and processed.	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 ApS' control activity*	*Grant Thornton's test*	*Result of test*
B.16	Backup copies of information software and system images are taken and tested regularly in accordance with an agreed backup policy.	We have inspected configuration of backup and we have inspected documentation for the setup. We have inspected that backup is monitored. We have inspected lists of backupfiles and we have inspected documentation for recovery test.	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 ApS' control activity*	*Grant Thornton's test*	*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.

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 ApS' control activity*	*Grant Thornton's test*	*Result of test*
C.3	The employees of the data processor are screened as part of the employment process.	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.	No deviations noted.
C.4	Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.	We have, by sample test, inspected that employees appointed during the assurance period have signed a confidentiality agreement. We have, by sample test, inspected that employees appointed during the assurance period 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.

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 ApS' control activity*	*Grant Thornton's test*	*Result of test*
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	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.
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 the assessment of the need for a DPO and ensured that the company has assessed the need for a DPO during the period.	No deviations noted.
C.9	The processor keeps a record of categories of processing activities for each data controller. Regularly – and at least annually – an assessment is made of whether the record of categories of processing activities for each controller should be updated.	We have inspected that the categories of processing contains the following information: • the name and contact details of the processor, and the data protection officer • the categories of processing carried out on behalf of each controller • where applicable, transfers of personal data to a third country or an international organisation • where possible, a general description of the technical and organisational security measures.	No deviations noted.

Control objective D - Return and deletion of personal data

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

No.	*Lessor Group ApS' control activity*	*Grant Thornton's test*	*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 inspected that documentation exists of personal data being 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 inquired into whether the agreed deletion or return of data has taken place for terminated data processing sessions during the assurance period.	We have been informed that no deletion or return of data has taken place for terminated data processing sessions during the assurance period, why we have not tested the effectiveness of the control. 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 ApS' control activity*	*Grant Thornton's test*	*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.	*Lessor Group ApS' control activity*	*Grant Thornton's test*	*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-processors, including requirements for sub-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-processors used. 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.	We have inspected that Lessor Group ApS has made use of a sub-processor which were not approved by or communicated in a timely manner to new Data Controllers from 20 October 2022 to 31 December 2022. No further deviations noted.
F.3	When changing the generally approved sub-processors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the data processor. When changing the specially approved sub-processors used, this has been approved by the data controller.	We have inspected that formalised procedures are in place for informing the data controller when changing the sub-processors used. We have inspected documentation that the data controller was informed when changing the sub-processors used throughout the assurance period.	We have inspected that Lessor Group ApS has made use of a sub-processor which were not approved by or communicated in a timely manner to new Data Controllers from 20 October 2022 to 31 December 2022. No further deviations noted.
F.4	The data processor has subjected the sub-processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	We have inspected the existence of signed sub-data processing agreements with sub-processors used, which are stated on the data processor's list. 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.	*Lessor Group ApS' control activity*	*Grant Thornton's test*	*Result of test*
F.5	The data processor has a list of approved sub-processors.	We have inspected that the data processor has a complete and updated list of sub-processors used and approved. We have inspected that, as a minimum, the list includes the required details about each sub-processor.	No deviations noted.
F.6	Based on an updated risk assessment of each sub-processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the sub-processor.	We have inspected that formalised procedures are in place for following up on processing activities at sub-processors and compliance with the sub-data processing agreements. We have inspected documentation that each sub-processor and the current processing activity at such processor are subjected to risk assessment. We have inspected documentation that information on the follow-up at sub-processors is communicated to the data controller so that such controller may plan an inspection.	No deviations noted.

Control objective 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 ApS' control activity*	*Grant Thornton's test*	*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 if there have been requests by the data controller for assistance in handing out, correcting, deleting, or restricting or providing information about the processing of personal data to data subjects in the assurance period.	We have been informed that the data processor has not received requests from data controllers in relation to data subjects' rights, why we have not tested the effectiveness of the control. No deviations noted.

Control objective I – Managing personal data breaches

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

No.	*Lessor Group ApS' control activity*	*Grant Thornton's test*	*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 inquired if any personal data breaches have occurred in the assurance period.	We have been informed that no personal data breaches have occurred, why we have not tested the effectiveness of the control. No deviations noted.

Control objective I – Managing personal data breaches

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

No.	*Lessor Group ApS' control activity*	*Grant Thornton's test*	*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: • 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. We have inspected documentation that the procedures available support that measures are taken to respond to the personal data breach.	No deviations noted.

Section 5: Supplementary information from Lessor Group ApS

The following supplementary information has not been subject to the audit performed by Grant Thornton.

Based on Grant Thornton's identified deviations in the ISAE 3000 statement, Lessor A/S and Danske Lønsystemer A/S (hereinafter referred to as Lessor Group) have the following supplementary information:

Under control activity B.8, Grant Thornton has found the following:

"We have observed that Workforce is supported by TLS 1.0 and TLS 1.1. No further deviations noted."

To this, Lessor Group states that in the new audit period, Lessor Group requires TLS 1.2 by default.

Under control activity B.12, Grant Thornton has found the following:

”We have from 63 samples observed that: 8 samples were not approved and 2 samples no segregation of duties was present. We have been informed that a risk assessment is performed for all changes to systems, databases and networks but that the risk assessment is not formally documented at this moment. No further deviations noted.”

To this, Lessor Group states that all changes to our applications are approved. Some, such as the 8 mentioned above, are approved informally and thus could not be documented. The procedure will be tightened up so that the documentation requirement can be met in the future.

During control activity B.13, Grant Thornton has found the following:

"We have observed that for 1 out of 13 samples no ticket of approval was available for access creation. We have observed that no formal review of user access rights has been performed for Danløn and LessorLøn. No further deviations noted".

To this, Lessor Group states that a new process has been developed to ensure approval of all new user access assignments. The observation is found for one user access assignment in the transition period between the new and old process.

Lessor Group can initially inform that this observation is about a small number of internal privileged admin users on the platform. These admin users are monitored on an ongoing basis and are terminated the moment the employee in question no longer has a work-related need for these rights.

During control activity F.2 and F.3, Grant Thornton has found the following:

"We have inspected that Lessor Group ApS has made use of a sub-processor which were not approved by or communicated in a timely manner to new Data Controllers from 20 October 2022 to 31 December 2022. No further deviations noted."

To this, Lessor Group states that we according to GDPR and the data processor agreement has informed and corrected this use of a sub-processor in the said period to all new impacted clients as data controllers.

PENNEO

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

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

Henrik Basso Reichsthaler Møller
Underskriver 1
Serienummer: e2bb9ab5-a11a-4b50-864e-8c58af066374
IP: 212.60.xxx.xxx
2023-08-07 07:57:43 UTC

Mit ID

Martin Brogaard Borup Nielsen
GRANT THORNTON,STATSAUTORISERET REVISIONSPARTNERSELSKAB
CVR: 34209936
Underskriver 2
Serienummer: 658bcd61-1988-4367-b3eb-215cfbbb49b0
IP: 82.192.xxx.xxx
2023-08-07 08:23:48 UTC

Mit ID

Kristian Lydolph
Underskriver 3
Serienummer: CVR:34209936-RID:43340328
IP: 62.243.xxx.xxx
2023-08-07 08:28:32 UTC

NEM ID