



revi-it

Building a safer society through compliance

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 June 2021 to 30 March 2022

May 2022

REVI-IT A/S | www.revi-it.dk
Højbro Plads 10, 1200 København K
CVR: 30 98 85 31 | Tel. 33 11 81 00 | info@revi-it.dk
www.dpo-danmark.dk | www.revi-cert.dk

Table of Contents

Section 1:	Lessor Group ApS' description of processing activity for the supply of Lessor Group ApS' services.....	1
Section 2:	Lessor Group ApS' statement	4
Section 3:	Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to Lessor Group ApS' data processing agreement with customers.....	6
Section 4:	Control objectives, controls, tests, and results hereof.....	9

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 includes Lessor A/S and Danske Lønssystemer 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.

Application systems in scope are: Danløn, LessorWorkforce, LessorLøn and LessorPortalen.

Our control objectives, including rules and procedures as well as implemented controls

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 ApS has a clear and transparent corporate structure and employs approximately 150 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 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.

Changes in the audit period

During the audit period, Swelön and Ilohngelhalt have been taken out of service and 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, Emly International, InterLogic Danmark ApS, ContractBook and SaPagi Aps. In addition, Danløn uses Bogholder-gruppen.dk and Db2data ApS. 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 June 2021 to 30 March 2022. 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 June 2021 to 30 March 2022.
 - (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 June 2021 to 30 March 2022. 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 June 2021 to 30 March 2022.
- 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, 11 May 2022
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 in their role as Data Controllers.

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 customers as data controllers throughout the period from 1 June 2021 to 30 March 2022 and about b+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, Emplify International, InterLogic Danmark ApS, ContractBook and SaPagi Aps. 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.

Auditor'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 behavior and ethical requirements applicable to Denmark.

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

Our 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.

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

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

Limitations of controls at a data processor

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.

Opinion

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

- (a) The Description fairly presents Lessor Group ApS' services as designed and implemented throughout the period from 1 June 2021 to 30 March 2022.
- (b) The controls related to the control objectives stated in the Description were appropriately designed throughout the period from 1 June 2021 to 30 March 2022, 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 June 2021 to 30 March 2022.

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' 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, 11 May 2022

REVI-IT A/S

Statsautoriseret revisionsaktieselskab



Henrik Paaske
Statsautoriseret revisor



Christian H. Riis
Partner, CISA,

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 June 2021 to 30 March 2022.

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 be 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	<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 ApS' control activity	Test performed by REVI-IT A/S	Result of test
A.1	<p>Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available.</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 the policy for handling personal data and ensured that it contains requirements that data processing is carried out only on instructions.</p> <p>We have inspected the policy and are ensured that it has been updated during the period.</p>	No deviations noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	We have – by sample test - inspected data processing agreement and by random sample ensured that the data processor only carries out the processing of personal data as shown in the 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.	<p>We have inspected procedures for handling instructions and ensured that unlawful instructions will be communicated to the data controller.</p> <p>We have inquired if there have been any instructions during the period that the data processor has deemed to be illegal.</p>	<p>We have been informed that there have been no instructions during the period that the data processor has deemed to be illegal, which is why we have not been able to test the effectiveness of the data processor's procedures.</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 ApS' control activity	Test performed by REVI-IT A/S	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 the information security policy and ensured that it is a requirement that security measures comply with data processing agreements.</p> <p>We have inspected the policy and ensured that it has been updated during the period.</p>	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 inquired into the evaluation of the IT risk profile within the period, and we have inspected documentation that this has been reviewed during the period.	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 – by sample test - inspected measures against malware.	No deviations noted.
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	<p>We have inquired into the policy for network controls.</p> <p>We have inspected the policy for network controls.</p>	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.	<p>We have inquired into the guidelines for segregation of networks.</p> <p>We have inquired into an overview of networks.</p>	No deviations noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	We have inspected differentiated access functions for selected applications.	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 – by sample test - inspected relevant capacity processes.	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	Test performed by REVI-IT A/S	Result of test
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	<p>We have inquired into the policy of using encryption, and we have – by sample test - inspected the use of cryptography.</p> <p>We have inquired into the policies for administering cryptographic keys, which support the company's use of cryptographic techniques.</p>	No deviations noted.
B.9	<p>Logging has been established in systems, databases, and networks.</p> <p>Logon data are protected against manipulation and technical errors and are reviewed regularly.</p>	<p>We have inquired into user activity logging.</p> <p>We have inspected samples of logging configurations.</p> <p>We have inquired about secure log information, and we have inspected the solution.</p> <p>We have inquired into procedures regarding logging of activities performed by system administrators and operators.</p> <p>We have inquired into procedures for clock synchronization, and we have inspected the solution.</p>	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.	<p>We have inspected the procedure for use of personal data in development and testing.</p> <p>We have – by sample test - inspected anonymised data in development.</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 the procedure for penetration tests.</p> <p>We have – by sample test - inspected penetration tests during the period.</p>	No deviations noted.

No.	Lessor Group ApS' control activity	Test performed by REVI-IT A/S	Result of test
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 inquired about the procedure regarding changes of information handling equipment and -systems.</p> <p>We have inquired into whether a selection of changes, made on platforms and databases have been approved, tested, documented, and implemented in the production environment, according to the change management procedure.</p>	No deviations noted.
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	<p>We have inquired into the procedure for creating and terminating users and we have inspected the procedures.</p> <p>We have inspected a sample of documentation for user creation and removal of users.</p> <p>We have inspected a sample of terminated employees and we have inspected whether their access rights have been revoked.</p> <p>We have inquired into the process of periodic review of users, and we have inspected checks for review.</p> <p>We have inquired into the procedure for the incorporation of rights, and we have inspected the procedure.</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.	We have – by sample test - inspected that access to personal data goes through 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.	<p>We have inquired into the procedures for access control to secure areas.</p> <p>We have inspected a sample of access points in order to establish whether personal access cards are used to gain access to production facilities.</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 ApS' control activity	Test performed by REVI-IT A/S	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 the information security policy and we have inspected documentation of management approval of the information security policy.</p> <p>We have inspected the procedure for periodic review of the information security policy.</p>	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 – by sample test - inspected that the requirements in data processing agreements are covered by the requirements of the information security policy for safeguards and security of processing.	No deviations noted.
C.3	The employees of the data processor are screened as part of the employment process.	<p>We have inquired into the procedure for employment of new employees and the security measures needed in the process.</p> <p>We have inspected a selection of contracts with employees in order to determine whether the procedure regarding background check has been followed.</p>	<p>We have observed that the screening process has not been performed as described in the HR procedure.</p> <p>No further deviations noted.</p>
C.4	Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.	We have inspected a selection of contracts with employees and consultants in order to determine whether these are signed by the employees.	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 inquired into the procedure for creating and terminating users and we have inspected the procedures.</p> <p>We have inspected a sample of terminated employees and we have inspected whether their access rights have been revoked.</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 ApS' control activity	Test performed by REVI-IT A/S	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 a selection of contracts with employees and ensured that confidentiality is still in effect.	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 inquired into procedures to secure adequate training and education (awareness training). We have inspected documentation for activities developing and maintaining security awareness with employees.	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 – by sample test - inspected the DPO's involvement during the period.	No deviations noted.
C.9	The processor keeps a record of categories of processing activities for each data controller.	We have inspected the record of processing.	We have observed that one of the records of processing has not been updated during the period. We have observed that the record of processing has subsequently been updated. No further 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	Test performed by REVI-IT A/S	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 the procedures for storing and deleting personal data in accordance with the agreement with the controller.</p> <p>We have inspected that the procedures are up to date.</p>	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 data processing agreement and ensured that storage and deletion has been agreed upon.	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 the procedures for processing the data controller's data at the end of the processing of personal data.</p> <p>We have – by sample test - inspected terminated customers and by random sample ensured that data has been returned or deleted.</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 ApS' control activity	Test performed by REVI-IT A/S	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 the procedures for storing and processing personal data only under 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 – by sample test - inspected data processing agreements and by random sample ensured that the data processor only processes data on approved locations.	No deviations noted.

Control objective F – Use of sub-processors

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

No.	Lessor Group ApS' control activity	Test performed by REVI-IT A/S	Result of test
F.1	Written procedures exist which include requirements for the data processor when using sub-data processors, including requirements for sub-data processing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected procedures for the use of sub-data processors, including requirements for sub-processing agreements and instructions. We have inspected that the procedures are up to date.	No deviations noted.
F.2	The data processor only uses sub-data processors to process personal data that have been specifically or generally approved by the data controller.	We have – by sample test - inspected data processing agreements and by sample test ensured that the sub processors have been approved by the controller.	No deviations noted.

Control objective F – Use of sub-processors

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

No.	Lessor Group ApS' control activity	Test performed by REVI-IT A/S	Result of test
F.3	When changing the generally approved sub-data processors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the data processor. When changing the specially approved sub-data processors used, this has been approved by the data controller.	We have inspected the procedures for informing the controller in the event of changes in the use of sub-processors. We have inquired about changes of sub-processors during the period.	No deviations noted.
F.4	The data processor has subjected the sub-data processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	We have inspected the list sub processors and inspected sub processor agreements.	No deviations noted.
F.5	The data processor has a list of approved sub-data processors.	We have inspected that the data processor has a comprehensive and up-to-date overview of used and approved sub processors.	No deviations noted.
F.6	Based on an updated risk assessment of each sub-data processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the sub-data processor.	We have inspected the ongoing checks of sub processors and ensured that the data processor has audited relevant sub processors.	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 ApS' control activity	Test performed by REVI-IT A/S	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 the policy for transfer of personal data.</p> <p>We have inspected that the policies are up to date.</p> <p>We have inspected that the processor has evaluated potential risks involving transfers to third countries.</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.	<p>We have inspected the policy for transfer of personal data.</p> <p>We have inspected data processing agreements.</p> <p>We have inspected the physical location for the servers.</p> <p>We have inquired about transfer of personal data to third countries.</p>	<p>We have been informed that the data processor does not transfer to third countries, and we find this probable based on our test actions.</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.	<p>We have inspected the policy for transfer of personal data.</p> <p>We have inspected data processing agreements.</p> <p>We have inspected the physical location for the servers.</p> <p>We have inquired about transfer of personal data to third countries.</p>	<p>We have been informed that the data processor does not transfer to third countries, and we find this probable based on our test actions.</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 ApS' control activity	Test performed by REVI-IT A/S	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.	We have inquired about a procedure enabling the company to assist the processor with requests concerning personal data, and we have inspected the procedures and descriptions for selected products.	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 inquired about documentation that requests for assistance from data controllers in relation to export, rectification and erasing of personal data in the audit period.	<p>The company states that no personal data requests have been registered during the audit period. Therefore, we have not been able to test the effectiveness of the procedures.</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 may be responded to in accordance with the data processing agreement entered into.

No.	Lessor Group ApS' control activity	Test performed by REVI-IT A/S	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 there are procedures 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 the procedures are up to date.</p>	No deviations noted.
I.2	The data processor has established controls to identify any personal data breaches.	We have inspected that the data processor provides awareness training to the employees in identifying any personal data breaches.	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-data processor.	We have inquired about security breaches during the period, and we have inspected documentation for, that relevant data controllers have been notified about relevant security breaches.	No deviations noted.
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 there are procedures established for informing the data controllers in the event of any personal data breach.</p> <p>We have inspected documentation for when a personal data breach occurred, measures were taken to respond to such breach.</p>	No deviations noted.