Independent service auditor's assurance report

Assurance engagement in relation to compliance with the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act for the delivery of Lessor Group's services as at 25-10-2019

ISAE 3000

Lessor Group

October 2019

REVI-IT A/S • state authorised public accounting firm
Jens Kofods Gade 1 • DK-1268 Copenhagen K • Phone 3311 8100 • info@revi-it.dk • revi-it.dk • CVR-no. 3098 8531

Table of contents

Lessor Group's statement

This assurance report concerns Lessor Group's services in relation to their compliance with the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act for services supplied to their customers.

Lessor Group supplies pay check services to their customers. We confirm that we, in our opinion, in all material respects have complied with the aforementioned criteria as at 25-10-2019.

We furthermore confirm that auditor has had access to all information and material necessary for issuing the assurance report.

On the basis of this it is our assessment that we, in all material respects, have conducted appropriate operations and administration of our services.

Allerød, 25-10-2019

Lessor Group

Peter Granild Colsted
CEO

Independent service auditor's assurance report on compliance with the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act as at 25-10-2019

To Lessor Group's management, the company's customers and their auditors

As agreed, we have reviewed Lessor Group's services in relation to their compliance with the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act as at 25-10-2019.

We did not perform any procedures regarding the operating effectiveness of controls included in the description and, accordingly, do not express an opinion thereon.

Our opinion is issued with reasonable assurance.

The assurance report is intended solely for the use of the management of Lessor Group, their customers and their auditors for assessing the existing procedures, and must not be used for other purposes.

Management's responsibility

Lessor Group's management is responsible for implementing and ensuring the maintenance of procedures in connection with their services as required by the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act.

Service auditor's responsibility

On the basis of the conducted work, it is our responsibility to express an opinion on whether the company's delivery in relation to Lessor Group's services complies with the requirements stated in the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act.

We have conducted our work in accordance with ISAE 3000, Assurance engagements other than audits or reviews of historical financial information and additional requirements under Danish audit regulation in order to obtain reasonable assurance for our opinion.

REVI-IT A/S applies International Standard on Quality Control 1 and accordingly 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.

We have complied with the independence and other ethical requirements of the Code of Ethics for professional Accountants issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

Our work comprised enquiries, observations as well as assessments and examination in spot checks of the information we have been provided.

Due to limitations in all control systems errors or fraud may occur, which might not be uncovered by our work. Also, the projection of our opinion on transactions in subsequent periods is subject to the risk of changes to systems or controls, changes to the requirements in relation to the processing of data or to the company's compliance with the described policies and procedures, whereby our opinion may not be applicable anymore.

Opinion

This opinion is formed on the basis of the understanding of the criteria accounted for in the assurance report's introductory section and which are based on the requirements in the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act.

It is our opinion that Lessor Group's delivery in connection with their services in all material respects has met the criteria mentioned as at 25-10-2019.

Description of tests of controls

The specific controls tested, and the nature, timing and results of these tests are listed in the subsequent main section.

Intended users and purpose

This assurance report is intended only for customers who have used Lessor Group's services, and their auditors, who have a sufficient understanding to consider the description along with other information, including information about controls operated by customers themselves in assessing compliance with the requirements of the General Data Protection Regulation.

Copenhagen, 25-10-2019

REVI-IT A/S
State authorised public accounting firm

Henrik Paaske
State Authorised Public Accountant

Martin Brogaard Nielsen
IT Auditor, CISA, CIPP/E, CRISC, CEO

Control objectives, controls, tests, and related test controls

The following overview is provided to facilitate an understanding of the effectiveness of the controls implemented by Lessor Group in the delivery of their services according to compliance with the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act. Our testing of functionality comprised the controls that we considered necessary to provide reasonable assurance for compliance with the specified articles as at 25-10-2019.

The requirements evident directly from the EU General Data Protection Regulation (GDPR) or the Danish Data Protection Act cannot be derogated from. However, it can be adjusted how the security is implemented, as the security requirements in GDPR in several respects are of more general and overall character that i.e. must consider purpose, nature of processing, category of personal data etc. In addition, there may be specific requirements in each customer contract that may have a scope extending beyond the general requirements of the Data Protection Act. If this is the case, these are not covered by the following.

Moreover, our assurance report does not apply to any controls performed at Lessor Group's customers, as the customers' own auditors should perform this review and assessment.

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

Method	General description
Inquiry	Interview, i.e. inquiry with selected personnel at the company regarding controls
Observation	Observing how controls are performed
Inspection	Review and evaluation of policies, procedures, and documentation concerning the performance of controls
Re-performing control procedures	We have re-performed – or have observed the re-performance of – controls in order to verify that the control is working as assumed

Control objective A – Instruction regarding the processing of personal data

Procedures and controls are observed that ensure that instruction regarding the processing of personal data is complied with in accordance with the entered processor agreement.

No.	Processor's control activity	Auditor's performed test	Test result
A.1	There are written procedures containing requirements that processing of personal data may only occur on the basis of an instruction.	We have inquired about documentation for the company only processing personal data based on instruction from the controller, and we have inspected controls for securing that processing is compliant with instructions.	No significant deviations noted.
A.2	The processor only performs the processing of personal data evident from the instruction from the controller.	We have inquired about documentation for management ensuring that the processing of personal data only occurs in accordance with the instruction and we have in spot checks inspected the data processing agreement. We have inspected controls for securing that data processing is compliant with instructions.	No significant deviations noted.
A.3	The processor immediately notifies the controller if an instruction according to the processor is contrary to the General Data Protection Regulation or data protection provisions in other EU law or the Member States' national legislation.	We have inquired about guidelines for managing unlawful instructions, and we have inspected documentation.	No significant deviations noted.

Control objective B – Technical measures

Procedures and controls are observed that ensure that the processor has implemented technical measures for ensuring relevant security of data processing.

No.	Processor's control activity	Auditor's performed test	Test result
B.1	There are written procedures containing requirements on the establishment of agreed security measures for the processing of personal data in accordance with the agreement with the controller.	We have inquired about documentation showing that the company's established security measures for the processing of personal data are in compliance with the agreed measures, and we have inspected processor agreements and the information security policy. We have inspected controls for securing that data processing is compliant with instructions.	No significant deviations noted.
B.2	The processor has performed a risk assessment and on the basis of this, has implemented the technical measures assessed to be relevant in order to achieve adequate security, including establishing the security measures agreed with the controller.	We have inquired about whether formalised procedures are in place ensuring that the processor performs a risk assessment in order to achieve adequate security, and we have inspected procedures and a product specific Data Privacy Impact Assessment.	No significant deviations noted.
B.3	Antivirus is installed on the systems and databases that are used for the processing of personal data, and the antivirus is updated regularly.	We have inquired about the use of antivirus on servers, and we have inspected an ISAE 3402 assurance report from the company concerning, i.a., controls related to the use of antivirus.	No significant deviations noted.
B.4	External access to systems and databases used for the processing of personal data occurs through a secured firewall.	We have inquired about the use of firewall for the protection of data, and we have inspected procedures for the use of firewall, as well as an ISAE 3402 assurance report from the company concerning, i.a., controls related to external access.	No significant deviations noted.

No.	Processor's control activity	Auditor's performed test	Test result
B.5	Internal networks are segregated in order to ensure restriction of access to systems and databases used for the processing of personal data.	We have inquired about whether internal networks are segregated in order to ensure restriction of access to systems and databases used for the processing of personal data, and we have inspected an ISAE 3402 assurance report from the company, network diagrams, and procedures for network security.	No significant deviations noted.
B.6	Access to personal data is isolated to users with a work-related need for this.	We have inquired about a procedure for the creation and deregistration of users, and we have inspected an ISAE 3402 assurance report from the company concerning, i.a., controls regarding access to data. We have inquired about documentation for different user rights and password policies on the company's services, and we have in spot checks inspected the implementation.	No significant deviations noted.
B.7	System monitoring with alarming has been established for the systems and databases used for the processing of personal data.	We have inquired about documentation for logging on the company's systems, and we have inspected an ISAE 3402 assurance report from the company concerning, i.a., controls regarding system monitoring.	No significant deviations noted.
B.8	Effective cryptography is used at the transmission of confidential and sensitive personal data via the Internet and via email.	We have inquired about the use of cryptography, and we have inspected an ISAE 3402 assurance report from the company concerning, i.a., controls regarding the use of cryptography.	No significant deviations noted.

No.	Processor's control activity	Auditor's performed test	Test result
B.9	Logging has been established in systems, databases, and networks, of the following matters: - Activities performed by system administrators and others with special rights - Security incidents Log information is protected against manipulation and technical errors and is reviewed regularly.	We have inquired about documentation for logging on the company's systems and services, and we have in spot checks inspected documentation for this.	No significant deviations noted.
B.10	Personal information used for development, testing or the like is always in pseudonymised or anonymised form. Use is made solely for the purpose of fulfilling the purpose of the person responsible under the agreement and on their behalf.	We have inquired about procedures for the use of personal data for development, testing and the like, which ensure that personal data is only used in pseudonymised or anonymised form, and we have inspected the procedure.	We have observed that the company does not have a formal policy for pseudonymising or anonymising test data based on production data. However, we have observed that the company has several measures in relation to data minimisation. No further significant deviations noted.
B.11	The established technical measures are regularly tested by means of vulnerability scans and penetration tests.	We have inquired about formalised procedures for ongoing testing of technical measures, including performing vulnerability scans and penetration tests, and we have inspected an ISAE 3402 assurance report from the company concerning, i.a., controls regarding vulnerability scans.	No significant deviations noted.

No.	Processor's control activity	Auditor's performed test	Test result
B.12	Changes to systems, databases, and networks are made in accordance with established procedures that ensure maintenance by means of relevant updates and patches, including security patches.	We have inquired about change management, and we have inspected an ISAE 3402 assurance report from the company, concerning, i.a., controls regarding change management.	We have observed in a spot check of the ISAE 3402 assurance report that no consideration has been made regarding the type of changes. The specific changes therefore did not meet the requirements of the procedure, including test and fallback plans. However, we have observed that the changes in question would have been classified as standard changes. No further significant deviations noted.
B.13	There is a formalised business process for assigning and interrupting user access to personal data. Users' access is regularly reassessed, including that rights can continually be justified by a work-related need.	We have inquired about formalised procedures for assigning and revoking users' access to systems and databases used for processing personal data, and we have inspected the company's assurance report. We have inquired about documentation for regular - at least annual - assessment and approval of assigned user access, and we have inspected documentation for the review.	No significant deviations noted
B.14	Access to systems and databases in which personal data is processed, which entails a high risk for the data subjects, is as a minimum by the use of two-factor authentication.	We have inquired about the company's high-risk processing.	The company has stated that there is no high-risk processing and in general, the company processes all data as classified data. No further significant deviations noted.
B.15	Physical access security has been established so that only authorised persons can gain physical access to premises and data centres in which personal information is stored and processed.	We have inquired about formalised procedures to ensure that only authorised persons can gain physical access to premises and data centres where personal information is stored and processed, and we have inspected an ISAE 3402 assurance report from the company concerning, i.a., controls regarding physical access.	No significant deviations noted.

Control objective C – Organisational measures

Procedures and controls are observed that ensure that the processor has implemented organisational measures for ensuring relevant security of data processing.

No.	Processor's control activity	Auditor's performed test	Test result
C.1	The processor's management has approved a written information security policy, which has been communicated to all relevant stakeholders, including the processor's employees. The information security policy is based on the performed risk assessment. Regularly – and at least annually – an assessment is made of whether the information security policy should be updated.	We have inquired about the preparation of an information security policy, and we have inspected the prepared information security policy. We have inquired about periodic review of the information security policy, and we have inspected documentation showing that the information security policy is updated.	No significant deviations noted.
C.2	The processor's management has ensured that the information security policy is not contrary to entered processor agreements.	We have inquired about documentation for the company ensuring that the information security policy is not contrary to agreed processor agreements, and we have inspected an assurance report from the company.	No significant deviations noted.
C.3	The processor's employees are checked in connection with employment.	We have inquired about a procedure for the recruiting and screening of new employees, and we have inspected the ISAE 3402 assurance report from the company concerning, i.a., controls regarding screening of new employees.	No significant deviations noted.
C.4	At employment, employees sign a confidentiality agreement. In addition, the employee is introduced to the information security and procedures regarding data processing as well as other relevant information in connection with the employee's processing of personal data.	We have inquired about confidentiality in the employment, and we have inspected a contract template and identified requirements to confidentiality in the employment relationship. Additionally, we have inspected an ISAE 3402 assurance report from the company concerning, i.a., the use of confidentiality agreements.	No significant deviations noted.

No.	Processor's control activity	Auditor's performed test	Test result
C.5	At the termination of employment, a procedure has been implemented at the processor ensuring that the user's rights are deactivated or terminated, including that assets are returned.	We have inquired about a procedure for offboarding employees, and we have inspected an ISAE 3402 assurance report from the company concerning, i.a., controls regarding the termination of employment. We have inquired about documentation for deregistration of users in connection with termination of employment, and we have inspected an ISAE 3402 assurance report from the company concerning, i.a., controls regarding the termination of employment.	No significant deviations noted.
C.6	At termination of employment the employee is informed that the signed confidentiality agreement still is applicable, and that the employee is subject to a general duty of non-disclosure in relation to the processing of personal data that the processor performs for the controllers.	We have inquired about a procedure for offboarding employees.	No significant deviations noted.
C.7	There is periodic awareness training of the processor's employees in relation to information security in general as well as security of data processing in relation to personal data.	We have inquired about awareness training, and we have inspected documentation for awareness training being conducted.	No significant deviations noted.

Control objective D – Return and deletion of personal data

Procedures and controls are observed that ensure that personal data can be deleted or returned if agreed with the controller.

No.	Processor's control activity	Auditor's performed test	Test result
D.1	There are written procedures containing requirements that storage and deletion of personal data occurs in accordance with the agreement with the controller.	We have inquired about a policy for the deletion of data, and we have inspected the policy. Additionally, we have inspected service guidelines from the company.	No significant deviations noted.
D.2	The specific requirements to the processor's storage period and deletion routines have been agreed.	We have inquired about processor agreements with customers, and we have inspected the template.	No significant deviations noted.
D.3	At the end of the processing of personal data for the controller, data is according to the agreement with the controller: - Returned to the controller, and/or - Deleted, where not in conflict with other legislation	We have inquired about a process for the deletion of data at the expiry of the agreement, and we have spot-checked product specific procedures for deletion/return at the expiry of requirements on documenting cases.	No significant deviations noted.

Control objective E – Storage of personal data

Procedures and controls are observed that ensure that the processor only stores personal data in accordance with the agreement with the controller.

No.	Processor's control activity	Auditor's performed test	Test result
E.1	There are written procedures containing requirements that storage of personal data only occurs in accordance with the agreement with the controller.	We have inquired about documentation for the processor only storing personal data in accordance with the processor agreements, and we have inspected documentation for this.	No significant deviations noted.
E.2	The processor's processing including storage must only take place at the locations, in the countries, or the territories approved by the controller.	We have inquired about documentation for the controller having approved the locations for processing, and we have inspected the processor agreements.	No significant deviations noted.

Control objective F – Use of sub-processors

Procedures and controls are observed that ensure that only approved sub-processors are used and that the processor when following up on their technical and organisational measures for protection of the rights of the data subjects and the processing of personal data ensures adequate security of data processing.

No.	Processor's control activity	Auditor's performed test	Test result
F.1	There are written procedures containing requirements to the processor at the use of sub-processors, including requirements on sub-processor agreements and instruction.	We have inquired about a procedure for supplier management, and we have inspected the procedure.	No significant deviations noted.
F.2	The processor solely uses sub-processors for the use of processing of personal data that are specifically or generally approved by the controller.	We have inquired about documentation for the company only using sub-processors for processing personal data that are specifically or generally approved by the controller, and we have inspected processor agreements.	No significant deviations noted.

No.	Processor's control activity	Auditor's performed test	Test result
F.3	In case of changes to the use of generally approved sub-processors, the controller is informed in a timely manner in order to be able to raise objections and/or withdraw personal data from the processor. In case of changes to the use of specifically approved sub-processors, this is approved by the controller.	We have inquired about a process for changes to sub-processors.	We have observed that the company does not have formal processes to ensure that data controllers approve new sub-processors. However, we have observed that the company has ensured that all sub-processors are mentioned in data processor agreements. No further significant deviations noted.
F.4	The processor has subjected the sub-processor to the same data protection obligations as those stated in the processor agreement or the like with the controller.	We have inquired about documentation for the sub-processor being subject to the same obligation as the processor, and we have inspected documentation for this.	No significant deviations noted.
F.5	The processor has a list of approved sub-processors	We have inquired about documentation for approved sub-processors being listed with adequate identification, and we have inspected a list of sub-processors.	No significant deviations noted.
F.6	On the basis of an updated risk assessment of each sub-processor and the activity taking place at this sub-processor, the processor performs periodic follow-up on this at meetings, inspections, review of assurance report, or similar.	We have inquired about documentation for the company performing periodic supervision and inspection of each sub-processor, and we have inspected audit questionnaire and audit letter to sub-processors.	No significant deviations noted.

Control objective G – Transfer of personal data to third countries

Procedures and controls are observed that ensure that the processor only transfers personal data to third countries or international organisations in accordance with the agreement with the controller on the basis of a valid ground for transfer.

No.	Processor's control activity	Auditor's performed test	Test result
G.1	There are written procedures containing requirements that the processor only transfers personal data to third countries or international organisations in accordance with the agreement with the controller on the basis of a valid ground for transfer.	We have inquired about whether data is transferred to third countries.	The company states that data will not be transferred to third countries (outside the EU/EEA) and that the company requires that their sub-processors do not transfer data to third countries (outside the EU/EEA) either. No further significant deviations noted.

Control objective H – Rights of the data subjects

Procedures and controls are observed that ensure that the processor can assist the controller with handing over, correcting, erasing, or the restriction of and providing information about the processing of personal data to the data subject.

No.	Processor's control activity	Auditor's performed test	Test result
H.1	There are written procedures containing requirements that the processor must assist the controller in relation to the rights of the data subjects. Regularly – and at least annually – an assessment is made of whether the procedures should be updated.	We have inquired about a procedure for the company being able to assist the processor with requests concerning personal data, and we have inspected the procedure. We have inquired about updating of the procedure and we have inspected that the procedure has been updated.	No significant deviations noted.
H.2	The processor has established procedures that to the extent agreed permits timely assistance to the controller in relation to handing over, correcting, erasing, or the restriction of and providing information about the processing of personal data to the data subject.	We have inquired about documentation for the possibility of right to access, and we have inspected documentation for the possibility of granting access. We have inquired about documentation for the possibility of erasing data, and we have inspected documentation for the possibility of anonymising data. We have inquired about documentation for the possibility of correcting data, and we have inspected documentation for correction of data being possible.	No significant deviations noted.

Control objective I – Managing personal data breaches

Procedures and controls are observed that ensure that any personal data breaches can be managed in accordance with the entered processor agreement.

No.	Processor's control activity	Auditor's performed test	Test result
I.1	There are written procedures containing requirements that the processor must inform the controller in case of personal data breaches. Regularly – and at least annually – an assessment is made of whether the procedures should be updated.	We have inquired about a procedure for managing personal data breaches, and we have inspected the procedure. We have inquired about updating the procedure and we have inspected that the procedure has been updated.	No significant deviations noted.
I.2	The processor has established the following controls for identification of any personal data breaches: - Employee awareness	We have inquired about training of employees to ensure correct management of personal data breaches, and we have inspected documentation for the training.	No significant deviations noted.
I.3	In case of a personal data breach the processor has informed the controller without undue delay after finding out that the personal data breach has occurred at the processor or a sub-processor.	We have inquired about personal data breaches, and we have inspected a breach log and a detailed description of the latest breach.	No significant deviations noted.

No.	Processor's control activity	Auditor's performed test	Test result
I.4	The processor has established procedures for assisting the controller at the controller's notification to the Danish Data Protection Agency (Datatilsynet): - The type of personal data breach - Probable consequences of the personal data breach - Measures taken or suggested to be taken in order to manage the personal data breach	We have inquired about a procedure for managing personal data breaches, and we have checked that the procedure considers: - Description of the type of personal data breach - Description of the probable consequences of the personal data breach - Description of measures taken or suggested taken in order to manage the personal data breach Additionally, we have inspected the procedure.	No significant deviations noted.

Control objective K – Record of processing activities

Procedures and controls are observed that ensure that the processor maintains a record of categories of processing activities performed on behalf of the controller.

No.	Processor's control activity	Auditor's performed test	Test result
K.1	The processor keeps a record of categories of processing activities for each controller, containing: - Name and contact information on the processor for each controller and – if relevant – the controller's Data Protection Officer - The categories of processing performed on behalf of each controller - Transfer of personal data to third countries or international organisations, and in case of transfers according to Article 49, paragraph 1, second subparagraph, documentation for adequate guarantees - A general description of the technical and organisational measures	We have inquired about the preparation of a record, and we have inspected the record.	No significant deviations noted.
K.2	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 inquired about periodic updating of the record.	No significant deviations noted.
K.3	Management has ensured that the record of categories of processing activities for each controller is adequate, updated, and correct.	We have inquired about documentation showing that management has ensured that the list of categories of processing activities for each data controller is complete, updated, and correct.	No significant deviations noted.