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' services in the role as data processor for the period 26-10-2019 to 31-03-2020

ISAE 3000

Lessor Group

May 2020

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

Section 1: Lessor Group's statement

Lessor Group processes personal data on behalf of data controllers under the Data Processor Agreements.

The enclosed description is prepared for use by data controllers who have used the services and who have sufficient understanding to evaluate the description together with other information, including information on controls, which the data controllers themselves performed by assessing whether the requirements of the EU' General Data Protection Regulation are complied with. Lessor Group confirms that:

a) The accompanying control description page gives a true and fair description of the services, which has processed personal data for data controllers covered by the data protection regulation throughout the period from 26-10-2019 to 31-03-2020. The criteria used to make this opinion were that the accompanying description:

(i) Describe how the services was designed and implemented, including:

- The types of services provided, including the type of processed personal data
- The processes in both IT and manual systems used to initiate, register, process and, if necessary, correct, delete, and restrict the processing of personal data
- The processes used to ensure that the data processing has been carried out in accordance with a contract, instruction, or agreement with the data controller
- The processes that ensure that the persons authorized to process personal data are bound by confidentiality or are subject to an appropriate statutory duty of confidentiality
- The processes that, upon discontinuation of data processing, ensure that at the discretion of the data controller, all personal data is deleted or returned to the data controller, unless law or regulation provides for the retention of personal data.
- The processes that, in the event of a breach of the personal data security, support that the data controller can report to the regulator and notify the data subjects
- The processes that ensure appropriate technical and organizational safeguards for the processing of personal data, taking into account the risks of processing, in particular through accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data transmitted right, stored or otherwise processed
- Controls that we have provided, with reference to the services, the delimitation of the data controllers and, if necessary, to achieve the control objectives that are listed in the specification, are identified in the specification
- Other aspects of our control environment, risk assessment process, information system (including the associated business processes) and communications, control activities and monitoring controls that have been relevant to the processing of personal data.

(ii) Contains relevant information on changes in the data processor's services for processing of personal information made during the period from 26-10-2019 to 31-03-2020.

(iii) Does not omit or distort information relevant to the scope of the Lessor Group services for processing personal data, taking into account that the description has been prepared to meet the general needs of a wide circle of data controllers and therefore cannot include every aspect of services, which the individual data controller must consider important according to their particular circumstances

b) The controls relating to the control objectives set out in the accompanying description were appropriately designed and effective throughout the period from 26-10-2019 to 31-03-2020. The criteria used to make this opinion were that:

   (i) The risks that threatened the achievement of the control objectives set out in the specification were identified

   (ii) The checks identified, if performed as described, would provide a high degree of assurance that the risks in question did not impede the achievement of the stated control objectives; and

   (iii) The controls were used consistently as designed, including manual checks carried out by persons of appropriate competence and authority throughout the period from 26-10-2019 to 31-03-2020.

c) Appropriate technical and organizational measures have been established and maintained to fulfilling the agreements with data controllers, good data processing practices and relevant data processing requirements under the Data Protection Regulation.

Allerød, 13-05-2020

Lessor A/S

Henrik Møller
CEO

Section 2: Lessor Group's control description of the services as well as internal controls

Introduction

Lessor Group consists of Lessor A/S, Danske Lønsystemer A/S, NORLØNN AS, Swelönn AB and ilohngehalt internetservices GmbH.

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, Lessor5, Lessor5 SaaS, Lessor App, LessorLøn, LessorLøn SaaS, Payroll to Microsoft Dynamics NAV, Human Resource to Microsoft Dynamics NAV, Time & Attendance to Microsoft Dynamics NAV, LessorPM HR, LessorPM Payroll, The Lessor Portal, LessorRefusion, Lessor SP Tid, Danløn, Norlønn, Swelön, ilohngehalt and LessorWorkforce.

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 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 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 made the choice not to appoint a 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. In order 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 asure that any unstructured data (eg. 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

There have been no significant changes in the data processor's services for processing of personal information during the audit period.

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 fulfill legislation

Section 3: Independent service auditor's assurance report on compliance with the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act for the period 26-10-2019 to 31-03-2020

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

As agreed, we have reviewed Lessor Group' Lessor A/S services in relation to their compliance with the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act for the period 26-10-2019 to 31-03-2020

Our opinion is issued with reasonable assurance.

The assurance report is intended solely for the use 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.

Limitations in controls at a data processor

Lessor Group description has been prepared to meet the common needs at a broad range of data controllers and may not, therefore, include every aspect of the services provided by Lessor Group, that each individual data controller may consider for important according to their specific circumstances. Also, because of their nature, controls at a processor may not prevent or detect all personal data breaches. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a controller may become inadequate or fail.

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 for the period 26-10-2019 to 31-03-2020

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. This information serves to obtain an understanding of the customers' information systems, which are relevant for compliance in the role as data processor in relation to EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act.

Copenhagen, 13-05-2020

REVI-IT A/S
State authorised public accounting firm

Henrik Paaske
State Authorised Public Accountant

Christian H. Riis
IT Auditor, CISA, Director

Section 4: 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 in the period for 26-10-2019 to 31-03-2020.

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
Inspection	Review and evaluation of policies, procedures and documentation concerning the performance of controls. This includes reading and assessment of reports and documents in order to evaluate whether the specific controls are designed in such a way, that they can be expected to be efficient when implemented.
Observation	Observing how controls are performed.
Inquiries	Interview with appropriate personnel at Lessor Group regarding controls.
Re-performance	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	REVI-IT'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. Regularly – and at least annually – an assessment is made of whether the procedures should be updated.	We have inquired about documentation for the company only processing personal data on the basis of instruction from the controller, and we have inspected a control from the company. We have inspected that the period control for the review of data processing agreements have been executed in the audit period.	No deviations noted.
A.2	The processor only performs the processing of personal data evident from the instruction from the controller.	We have inspected Data Processing Agreements for selected products. We have inspected a control ensures that the processing of personal data only occurs in accordance with the instruction.	No 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. We have inspected standard Data Processing Agreements for selected products.	No 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	REVI-IT'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. Regularly – and at least annually – an assessment is made of whether the procedures should be updated.	We have inquired about documentation showing that the company's established security measures for the processing of personal data is in compliance with the agreed measures, and we have inspected the control for the review of data processing agreements. We have inspected that the period control for the review of data processing agreements has been executed in the audit period.	No 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 inspected that a general risk assessment has been established with the support of DPIA's (Data Privacy Impact Assessments) for all products in Lessor Group. We have inspected that the performed risk assessment and DPIA's are updated and comprise the actual processing of personal data.	No 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 a policy for the use of antivirus, and we have inspected the 3402-audit report from Lessor Group, where this control is examined. We have inquired about the use of antivirus on servers, and we have inspected the 3402-audit report from Lessor Group, where this control is examined.	No 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 the 3402-audit report from Lessor Group, where this control is examined. We have inquired about the use of VPN when accessing data, and we have inspected the 3402-audit report from Lessor Group, where this control is examined.	No deviations noted.

No.	Processor's control activity	REVI-IT'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 whether internal networks are segregated in order to ensure restriction of access to systems and databases used for the processing of personal data. We have inspected network diagrams and a 3402-audit report from Lessor Group, where this control is examined.	No deviations noted.
B.6	Access to personal data is isolated to users with a work-related need for this.	We have inquired about internal access procedures, and we have inspected the 3402-audit report from Lessor Group. We have inspected differentiated access functions for selected applications/products. We have inspected the setup for password complexity for selected applications/products.	No 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 into whether system monitoring with alarming has been established for the systems and databases used for the processing of personal data, and we have inspected a 3402-audit report from Lessor Group, where this control is examined.	No 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 a policy for transmitting data via email, and we have inspected the policy. We have inquired about the use of cryptography in the company's ticket system, and we have inspected selected SSL-reports and a 3402-audit statement, where this control is examined.	No deviations noted.

No.	Processor's control activity	REVI-IT's performed test	Test result
B.9	Logging has been established in systems, databases, and networks. 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 we have inspected the 3402-audit report from Lessor Group, where this control is examined We have inspected documentation for logging in selected applications/products.	No deviations noted.
B.10	Personal information used for development, test or similar, are always in pseudonymised or anonymised form. Usage is only in order to perform the controller's purpose according to agreement and on its behalf.	We have inquired about the use of personal information for development, test and similar, and we have inspected an action plan from the company.	We have observed that the company does not have formal procedures and controls for pseudonymizing, or anonymizing test data based on production data. However, we have observed that the company have prepared an action plan with final implementation Q2 2020. No further deviations noted.
B.11	The established technical measures are regularly tested by means of vulnerability scans and penetration tests.	We have requested formalized procedures for ongoing testing of technical measures, including conduct of vulnerability scans and penetration tests, and we have inspected the 3402-audit report from Lessor Group, where this control is examined.	No deviations noted.
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 patch management, and we have inspected documentation for the management of a selected change in the 3402-audit report from Lessor Group, where this control is examined.	No deviations noted.

No.	Processor's control activity	REVI-IT's performed test	Test result
B.13	There is a formal procedure for allocating and revoking user accesses to personal data. Users' accesses are regularly reviewed, including that rights still can be justified by a work-related need.	We have inquired whether there are formalized procedures for the allocation and revoking of users' access to systems and databases that are used for the processing of personal data, and we have inspected the 3402 audit report from Lessor Group, where this control is examined. We have inquired whether there is documentation for regular – at least annual – assessment and approval of allocated user accesses, and we have inspected the 3402-audit report from Lessor Group, where this control is examined.	No deviations noted.
B.14	Access to systems and databases, in which personal data is processed, which entails a high risk for the data subjects, occurs as a minimum by means of two factor authentication.	We have inquired whether there are formalized procedures that ensure that two factor authentication are used at the processing of personal data which entails a high risk for the data subjects. We have inspected the 3402-audit report from Lessor Group, where this control is examined.	No deviations noted.
B.15	Physical access security has been established such that only authorised persons can gain physical access to premises and data centres in which personal data are stored and processed.	We have inquired whether there are formalized procedures that ensure that only authorized persons can gain physical access to premises and data centres in which personal data are stored and processed, and we have inspected the 3402 audit report from Lessor Group, where this control is examined.	No 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	REVI-IT'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 management approval and periodic review of the information security policy, and we have inspected the 3402-audit report from Lessor Group, where this control is examined.	No 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 the controls from the company.	No 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. We have inquired about documentation for screening of the most recent employees. We have inspected the 3402-audit report from Lessor Group, where this control is examined	No 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 relationship. We have inquired about staff training, and we have inspected documentation for staff training. We have inspected the 3402-audit report from Lessor Group, where this control is examined	No deviations noted.

No.	Processor's control activity	REVI-IT'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. We have inquired about documentation for de-registration of user in connection with the latest termination of employment. We have inspected the 3402-audit report from Lessor Group, where this control is examined.	No 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, and we have inspected the procedure and a 3402-audit report from Lessor Group, where this control is partly examined.	No 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 execution of awareness training, and we have inspected documentation for execution of GDPR-awareness training, and we have inspected the 3402-audit report from Lessor Group, where this control is partly examined.	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 inquired about whether the company has designated a DPO. We have inspected the company's assessment to the duty of having a DPO.	No 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	REVI-IT'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 controls for timely deletion of data, and we have inspected documentation for controls for timely deletion of data. We have inquired about a procedure for the deletion of data, and we have inspected descriptions of the procedures for selected applications.	No deviations noted.
D.2	Specific requirements to the processor's storage period and deletion routines have been agreed.	We have inspected data processor agreements with customers. We have inquired about decision on data retention.	The company states that, as a general rule, data is not continuously erased on behalf of the customer without specific instructions. No 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: J Returned to the controller, and/or J Deleted, where not in conflict with other legislation	We have inquired about a process for the deletion of data at the expiration of the agreement, and we inspected the procedures for selected products. We have inspected a sample of 25 customers discontinued during the audit period, in order to review whether there is that data is stored, returned or deleted in accordance to the policy. We have inspected deletions logs for selected products.	No 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	REVI-IT'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 inspected a control for the processor only storing personal data in accordance with the processor agreements.	No 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 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	REVI-IT'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 inspected a control for ensuring that the company only uses sub-processor mentioned in the agreement.	No 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 that the company is only using sub-processors for processing personal data that are specifically or generally approved by the controller, and we have inspected processor agreements and further documentation.	We have observed that the company had not informed the data controllers about the use of one data processor in the audit period. However, we have observed that the company have informed the data controllers after the audit period. We are further informed that the sub-processor in question was only used for 2 on-premise solutions. No further deviations noted.

No.	Processor's control activity	REVI-IT'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 information to data controllers regarding new sub-processors. No further 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 in spot checks inspected documentation for this.	No deviations noted.
F.5	The processor has a list of approved sub-processors.	We have inspected documentation for approved sub-processors being listed.	No 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 documentation for supervision.	No 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	REVI-IT'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. Regularly – and at least annually – an assessment is made of whether the procedures should be updated.	We have inquired about whether data is transferred to third countries, and we have been informed that all data is located in the EEA/EU.	We have been informed that all data is located in the EEA/EU. No 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	REVI-IT'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.	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 procedures and descriptions for selected products.	No 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 that requests for assistance from data controllers in relation to export, rectification, erasing and disclosure of processing of personal data in the audit period.	The company states that no personal data requests have been registered during the audit period. Therefore, we have not been able to test the procedures. No 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	REVI-IT'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 inspected a procedure for managing personal data breaches. We have inspected that the procedure is updated. We have inspected that the process for managing personal data breaches 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	No deviations noted.
I.2	The processor has established the controls for identification of any personal data breaches.	We have inquired about the controls to sufficient response to personal data breaches, and we have inspected a 3402-audit report from the company, where various controls have been examined.	No 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 documentation for the company's response to the breaches in the period.	No 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	REVI-IT'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 inspected an article 30 record from the company.	No 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 inspected documentation for the record being updated.	No 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 inspected documentation for the record being approved by the management.	No deviations noted.