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 in the role as data processor for the period 21-06-2019 to 31-05-2020

ISAE 3000

SpeedAdmin ApS

CVR-no.: 34 59 01 76

June 2020

Table of contents

Section 1: SpeedAdmin ApS' statement

The enclosed description is prepared for use by data controllers, who have used services and who have sufficient understanding to evaluate the description together with other information, including information of controls, which the controllers themselves performed by assessing whether the requirements of the EU' Regulation about the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (hereafter referred to as "General Data Protection Regulation")

SpeedAdmin 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 SpeedAdmin 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 used to ensure, that the persons, authorised to process personal data, have committed themselves to a non-disclosure agreement or are subject to adequate statutory professional 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 SpeedAdmin, 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 about changes in the data processor's SpeedAdmin for processing of personal information, made during the period 21-06-2019 to 31-05-2020

(iii) Does not omit or distort information relevant to the scope of the described SpeedAdmin 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 SpeedAdmin, 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 21-06-2019 to 31-05-2020. 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 21-06-2019 to 31-05-2020

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.

Sønderborg, 29 June 2020

Torben Dueholm Rasmussen

Co-founder

Karsten G. Rasmussen

Co-founder

Section 2: SpeedAdmin ApS' control description ISAE 3000

The purpose of the data processor's processing of personal data on behalf of the data controller is: To supply the administration system SpeedAdmin to schools of music and culture.

It is the schools of music and culture, who are responsible for supplying the data they need to be able to perform the daily administrative operational tasks in SpeedAdmin. This makes the schools of music and culture data controllers in relation to the data subjects.

The processing of personal data is performed according to the general agreement (license agreement) between SpeedAdmin and the schools of music and culture, which is signed in the beginning of the consignment.

The system is a 100% web based and need therefore not be retrieved or downloaded to the PC used. It is, however, an option to download the SpeedAdmin App to smartphones and tablets, to be used by teachers, students, and guardians.

Description of processing

The processors' processing of personal data on behalf of the controller is solely performed according to controller's instructions. Processor does not use personal data for other purposes, that then ones described in the controller's instructions.

Personal data

- CPR-number (DK) and "personnummer" (NO and SE)
- Data of birth (UK and DE)
- Address, postal code
- Full name
- E-mail
- Mobile- and telephone number

Categories of data subjects included in the data processor agreement:

- Schools of music and culture's employees
- Students
- Guardians
- If required, schools of music and culture's partner's liaison officers.

Practical measures

The management of SpeedAdmin has approved all measures, internal standards, individual yearly audits, performed internally within SpeedAdmin.

Every SpeedAdmin employee has been informed about personal data and information security. Annually, an internal security awareness training is being held, reviewing internal standards and information connected to GDPR and IT-security. All standards are accessible to all employees. In case of major changes in standards, all employees are being informed.

The system performs automatic logs. Among other things, all logins to the system, included failed logins are being logged. Changes made to students, guardians and teachers are being logged. Furthermore, searches for specific data subjects are also being logged.

Development of the system, which can have an impact on the rights of the data subjects are being registered in a log and SpeedAdmin's DPO is involved in the process. Potential security incidents and the handling of the are being registered. Annually, this log will be reviewed, focusing on the way the security incidents were handled.

Risk assessment

SpeedAdmin ApS has made a risk assessment of potential threats to the system and data security. The threats have been assessed, based on the probability of the threat occurring and how big an impact the threat would have, if real.

This risk assessment is reviewed minimum once a year. This review is focusing on, whether new threats have appeared since last review. Furthermore, the risk assessment is being adjusted, if measurements have been realized of if new possible solutions have been suggested.

Changes in the risk assessment will always be approved and signed by one of SpeedAdmin's managers.

Processing - instructions

In the data processor agreement, we have with our customers, the customers' instructions are described in connection with the data processing. We exclusively process data, based on these instructions.

We have a standard of, how we handle unlawful instructions, if such is received from a customer. All employees are familiar with this standard, and are able to act accordingly, in case they receive an unlawful instruction from a customer.

We also keep an article 30-record of the different processing of personal data performed by us – both in the role as data processor (on behalf of our customers) and as data controller (for our sub-suppliers). This record is also available to the employees, enabling them to keep informed. The article 30-record is reviewed at least once a year, in the beginning of the new year, or when needed. Reminders have been set up for those responsible, sending them a reminder of the review.

Apart from the article 30-record, we also manage user accesses for all employees. We have a list of all employees' user accesses, which will be updated whenever changes occur.

Procedure review

Once a year, or when needed, all internal standards are being reviewed. Additionally, various lists and logs are being examined and reviewed. This way we can form a general view of the general handling of the actual cases and decide whether changes to one or more standards are needed. At our yearly security awareness training day, all employees are asked to delete emails and other documents containing personal data.

Procedures – access management

SpeedAdmin's management is in charge of decisions and the administration of which user accesses the individual employee should have.

All accesses are being recorded in a document. This document is being updated with every change made in connection with accesses.

Personal access codes exist for both the employees' computer and the system itself.

All Speed Admin's employees have access to the office in Sønderborg. Everybody has received a key card with individual access codes, required for access during off-hours. Every key card is marked with a number, recorded in the access document for each employee.

Upon termination of an employee, the going standard must be complied with, in connection with return of key card and termination of the different accesses held by the individual.

Users are grouped by rights in the system. This means that not everybody has the same rights in the system, since the groups determines, which functions should be available to the individual. Apart from the groups in the system, all actions and by whom, are logged in the system.

Procedures – development

The internal standard including development of new or existing features, which can or will influence the rights of the data subjects and/or personal data, must be complied with. The procedure states, that the developers working on the individual cases, must record all in an internal log.

In addition to logging the developing, the DPO must also be involved before the development is being deployed (implemented into the system). DPO must be part of ensuring that the data subjects are protected in the best way possible and in accordance to the general data protection regulation.

Procedures – managing personal data requests

SpeedAdmin is not allowed to process personal data requests from data subjects. Since we are "only" the processor and therefore not data controller, we are not authorised to process these requests.
It is the role of the data controller – our customers, who are authorised to process personal data requests.

Therefore, we hardly ever receive similar orders. Since this however, is no guarantee that we won't get one, our standard includes a paragraph about the rights of the data subjects.

In case we receive a personal data request from a data subject, we refer the concerned to the relevant school. In addition, we log the request, that also will be reviewed when needed or at least once a year, in order for us to determine whether any part of the standard need to change.

Procedures – security incidents

SpeedAdmin ApS is logging security incidents according to the internal standard about security incidents. Amon other things, it is important that the DPO is included as soon as a security incident has been discovered.

In case of a security incident occurring, this must be logged, including information about, how the matter has been handled. This must be updated regularly – from the detection of the incident, until the case has been completed.

This log is reviewed annually. The review focuses on the management of last years' incidents, during this review, focus is among other things on the handling of the incident and on whether the standard need to be adjusted. If the standard is being adjusted, every employee will be notified.

Sub-processors

We have chosen to use sub-processors, since it is our opinion, that they contribute to the best combined solution for our customers.

The sub-processors are required – at any given time – to have adequate protection against electronical or physical unlawful access, malicious damage, theft, hacking, computer virus, denial of service attacks or other similar security incidents. Additionally, they must be protected from the risk of fire, storm, water damage or other similar circumstances, which can compromise SpeedAdmin's ability to fulfil contract requirements.

The sub-processors are reviewed once a year. We obtain the IT audit report if any is available. Failing this, we forward an annual questionnaire, describing their methods and procedures in securing a high degree of IT-security.

All non-confidential documents can, upon request, be forwarded to the data controller in connection with our review.

Third countries

It has been decided that SpeedAdmin neither store nor transfer data to third countries. Therefore, this is also an issue for inspection, before SpeedAdmin decides to employ a new sub-processor.

Employees

Upon onboarding a new employee, the IT-security policy and the internal standards are being reviewed. Apart from this the employee must sign a statement, which is included in our IT-security policy. The standard will be followed upon termination of employment.

Significant changes during the period

We have migrated from Gmail to Microsoft Outlook Apart from that, no significant changes have been made during the period.

Complementary controls

- Data controller is responsible for deleting the log
- Superusers are the only ones authorized to anonymize users in the system
- In case the controller downloads Excel spreadsheets from SpeedAdmin, the controller is responsible for deleting it
- The controller must pay attention to the mails being sent by the system about locked users

The controllers themselves have duty of disclosure to the data subjects in SpeedAdmin – we of course assist with information about the processing.

Section 3: Independent service auditor's assurance report on compliance with the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act in the role of data processor, 21-06-2019 to 31-05-2020

To SpeedAdmin ApS, the company's customers, and their auditors.

As agreed, we have reviewed SpeedAdmin ApS' services in relation to their compliance with the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act for the period of 21-06-2019 to 31-05-2020.

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

Management's responsibility

Speed Admin'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

SpeedAdmin's 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 SpeedAdmin, 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 SpeedAdmin ApS, in all material respects has met the criteria mentioned for the period 21-06-2019 to 31-05-2020

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 SpeedAdmin'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.

København, 29 June 2020

REVI-IT A/S
State authorised public accounting firm

Henrik Paaske
State authorised auditor

Basel Rimon Obari
IT-revisor, CISA, CISM, Partner

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 SpeedAdmin ApS 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 21-06-2019 to 31-05-2020.

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 SpeedAdmin's customers, as the customers' own auditors should perform this review and assessment.

We performed our tests of controls at SpeedAdmin 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 inspected the information security policy, and ensured that decisions have been made, to ensure that the processing of personal data only is performed in accordance with instructions. We have inspected, that procedures have been updated during the audit period. We have, by sample test, inspected new data processor agreements, and ensured that the requirements for instructions have been described.	No deviations noted.
A.2	The processor only performs the processing of personal data evident from the instruction from the controller.	We have, by sample test, inspected data processor agreements, and ensured that the processor complies with the instructions.	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 into, whether unlawful instructions have occurred during the audit period.	We have been informed, that no unlawful instructions have occurred during the audit period, wherefore we are not able to test the efficiency of the control. No further 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.	We have inquired about information security policy and ensured that decisions have been made to establish agreed security measures to protect personal data processing. We have, by sample test of 4 data processor agreements, ensured that the agreed security measures have been established.	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 the risk assessment and ensured that it is based on the rights of the data subjects. We have inspected the risk assessment and ensured that it has been updated during the audit period.	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, by sample test, inspected the implementation of protection against malware, and we have ensured the these have been properly configured and are regularly updated.	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, by sample test, inspected the implementation of firewall, including the rules for in-/outbound rules. We have inspected statement from operations supplier and ensured that firewalls have been installed.	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 inspected the list of networks and ensured that environments are segregated. We have inspected statement from operations supplier and ensured that the network is adequately segregated.	No deviations noted.
B.6	Access to personal data is isolated to users with a work-related need for this.	We have inspected, that formalized procedures for limiting user access to personal data, have been established. We have, by sample test, inspected the access rights of new employees during the audit period and ensured, that these are based on a work-related need.	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, by sample test inspected monitoring of system capacity, and ensured that this is done regularly.	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 inspected the policy for encryption and ensured that this addresses the transmission of personal data. We have, by sample test, inspected SSL Certificates and ensured that these have been appropriately configured.	No deviations noted.
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 inspected the policy for logging and ensured that decisions have been made to protect personal data. We have, by sample test, inspected the set-up of systems logging and we have ensured that this complies with the policy. We have, by sample test, inspected access to logfiles, and ensured that access is limited to a work-related need.	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, by sample test, inspected the development server and ensured that the data set is anonymized.	No deviations noted.

No.	Processor's control activity	REVI-IT's performed test	Test result
B.11	The established technical measures are regularly tested by means of vulnerability scans and penetration tests.	We have inquired about formalized procedures for regular testing of technical measures. We have inspected statement from operations supplier and ensured that regular patching of the operating system is performed.	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 inspected the procedure for changes and ensured that the rights of the data subjects are being taken into account. We have, by sample test, inspected changes during the audit period, and ensured that this have been performed according to the procedure.	No deviations noted.
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 inspected that formalized procedures are available for allocating and revoking of user access to systems and databases, used to process personal data. We have by sample test, inspected accesses, and ensured that new employees have been allocated according to the procedure. We have, by sample test, inspected accesses and ensured that terminated employees' access rights have been revoked according to the procedure. We have inspected that documentation is available of regular – and minimum once a year – review and approval of allocated user accesses.	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 about whether the company uses two factor authentication.	We have been informed, that SpeedAdmin is not processing sensitive personal data, wherefore SpeedAdmin has decided not to use two factor authentification. We have ensured, that VPN is being used when connecting to internal networks. No further 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 inspected the policy of physical security and ensured that physical security has been decided upon. We have inspected statement from operations supplier and ensured that physical securing of servers have been established.	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 inspected that information security policy is available, reviewed and approved by management within the audit period. We have ensured, that the information security policy is available to the employees. We have inspected the control of information security policy and ensured that this is regularly assessed.	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, by sample test, inspected data processor agreements, and ensured that the information security policy complies with the agreements.	No deviations noted.
C.3	The processor's employees are checked in connection with employment.	We have, by sample test, inspected new employments and ensured that the employment has followed the procedure for employments.	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, by sample test, inspected employment contracts of new employees during the audit period, and ensured that they have committed themselves to a confidentiality agreement. We have, by sample test, inspected statements, signed by new employees during the audit period, and ensured that they have confirmed having read the company policies and procedures.	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 inspected procedures to ensure that offboarding employees' access rights are deactivated or expires upon termination, and that assets such as key cards, PC, mobile phones etc. are being returned. We have, by sample test, inspected the termination of access and return of assets from former employees and ensured that this has been performed according to the procedure.	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, by sample test, inspected confidentiality agreements, and ensured that these still are applicable after termination of employment.	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, by sample test, inspected material from awareness training during the audit period, and we have ensured that this training is related to IT-security.	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 controls and procedures and ensured that the DPO has been involved.	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 inspected the information security policy and ensured that decisions have been made, how deletion is being performed according to agreements. We have inspected the procedure for deletion and ensured that this has been updated during the audit period. We have inspected the control of the procedure and ensured that the procedure is being regularly updated.	No deviations noted.
D.2	Specific requirements to the processor's storage period and deletion routines have been agreed.	We have, by sample test, inspected new data processor agreements, and ensured that decisions have been made about storage periods and deletion routines.	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: - Returned to the controller, and/or - Deleted, where not in conflict with other legislation	We have inspected that formalized procedures are available, describing the processing of the datasubjects' data upon termination of personal data processing. We have, by sample test of one data processing terminated during the period, ensured that documentation of deletion or return of data, is available.	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. Regularly – and at least once a year - assessment is made of whether the procedures need to be updated.	We have inspected the information security policy, and we have ensured that decisions have been made about storage of data. We have inspected the policy and ensured that this has been updated during the audit period.	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 inspected the data processor agreements and ensured that the storage location is according to the agreements. We have, by sample test, inspected the list of backups during the audit period and by sample test, ensured that these have been correctly configured.	We have observed that backup has not been configured according to the data processor's policy during the audit period. We have subsequently received documentation that this has been corrected. No further 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 Regularly – and at least once a year – an assessment is made, whether the procedures need to be updated.	We have inspected the policy of requirements of sub-processors and ensured that decisions have been made about sub-processor agreements. We have inspected that the policy has been updated during the audit period.	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, by sample test, inspected new data processor agreements during the audit period, and ensured that the processor either has a general or a specific authorization to use sub-processors.	No deviations noted.
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 changes of sub-processors during the audit period, and we have, by sample test, inspected that data controllers have been informed.	No 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 inspected data processor agreements with new sub-processors and ensured that the sub-processor is committed to same or similar data protection obligations as the controller.	No deviations noted.

No.	Processor's control activity	REVI-IT's performed test	Test result
F.5	The processor has a list of approved sub-processors.	We have inspected the list of sub-processors and ensured that all relevant sub-processors are stated in the list.	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, by sample test, inspected that regular review of sub-processors has been performed, and ensured that it has been done according to the procedure.	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 inspected written procedure containing requirements that personal data cannot be transferred to third countries, without instructions from data controller. We have inspected documentation that the procedure has been updated during the audit period.	We have been informed and has observed that data are not transferred to third countries, wherefore the control is not regarded to be relevant. No deviations noted.
G.2	The processor can only transfer personal data to third countries or international organizations, based on the controller's instructions.	We have, by sample test, inspected data processor agreements with new controllers during the audit period for instructions of transfer to third countries and we have ensured that decisions have been made about transfers to third countries.	No deviations noted.
G.3	In connection with transfers of personal data to third countries or international organizations, the data processor has assessed and documented, that transfers are based on valid grounds.	We have, by sample test, inspected data processor agreements with new data controllers during the audit period, for instructions about transfer to third countries.	We have been informed and has observed that data are not transferred to third countries, wherefore the control is not regarded to be relevant. 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. Regularly – and at least annually – an assessment is made of whether the procedures should be updated.	We have inspected the procedure for managing requests and ensured that decisions have been made about assisting the data controller. We have inspected the procedure and ensured that this has been updated during the audit period.	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, by sample test, inspected requests during the audit period, and we have ensured that these have been handled according to the procedure.	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 the procedure for personal data breaches and ensured that decisions have been made about informing the controller in case of personal data breaches. We have inspected the procedure and ensured that this has been updated during the period. We have inspected controls and ensured that security breaches are being reviewed regularly.	No deviations noted.
I.2	The processor has established the controls for identification of any personal data breaches.	We have inspected, that the processor is offering awareness training to the employees in relation to the identification of potential personal data breaches.	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 inspected the log of personal data breaches during the audit period.	We have observed that no personal data breaches have been detected during the audit period, wherefore we have not been able to test the efficiency of the procedure. No further deviations noted.
I.4	The processor has established procedures for assisting the controller when filling a report with the Danish Data Protection Agency.	We have inspected the procedure and ensured that assistance to the controller has been established.	We have observed that no personal data breaches have been detected during the audit period, wherefore we have not been able to test the efficiency of the procedures. No further deviations noted.

Control objective J – Conditions for consent and duty of disclosure

Procedures and controls are observed that ensure that the data subjects have given written consent to the processing of personal data, and in which it is ensured that the data subject has received the controller's contact information, information on the purpose of the processing of the personal data, as well as other information that is necessary for observing the duty of disclosure.

No.	Processor's control activity	REVI-IT's performed test	Test result
J.1	There are written procedures for the obtaining of written consent for the processing of personal data.	We have inquired about the handling of consent and duty of disclosure.	We have been informed that the company is not obtaining consent from the data subjects in connection with revised services, wherefore this point is not relevant. No further 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.	We have inspected the record and ensured that it complies with the requirements of the statutory regulation.	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 the record and ensured that it has been updated during the audit period.	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 the record and ensured that management has approved the record.	No deviations noted.