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 processor

ISAE 3000

Speedware ApS

CVR-no.: 34 59 01 76

June 2019

Table of contents

Speedware ApS' statement

This assurance report concerns Speedware ApS' compliance with the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act.

We confirm that we, in our opinion, in all material respects have complied with the aforementioned criteria as at 20-06-2019.

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.

Sønderborg, 20 June 2019

Speedware ApS

Torben Dueholm Rasmussen
Co-founder and CEO

Karsten Grau Rasmussen
Co-founder and CTO

Independent service auditor's assurance report on compliance with the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act as at 20-06-2019

To Speedware ApS' management, the company's customers and their auditors

As agreed, we have reviewed Speedware ApS' compliance with the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act as at 20-06-2019.

Our opinion is issued with reasonable assurance.

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

Management's responsibility

Speedware ApS' management is responsible for implementing and ensuring the maintenance of procedures 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 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 inquiries, 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 Speedware ApS in all material respects has met the criteria mentioned as at 20-06-2019.

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 and description of test of controls is intended only for controllers who have used Speedware ApS' services, and their auditors, who have a sufficient understanding to consider the description along with other information, including information about controls operated by the controllers themselves when assessing whether the requirements in the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act have been complied with.

Copenhagen, 20 June 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 create an overview of the controls implemented by Speedware ApS in relation 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 20-06-2019.

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 Speedware ApS' customers, as the customers' own auditors should perform this review and assessment.

We performed our tests of controls at Speedware ApS 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. 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 processor agreements and information security policy. Additionally, we have inquired about ongoing updating of the policy, and we have inspected control for ongoing updating of the information security policy.	No significant deviations noted.
A.2	The processor only performs the processing of personal data evident from the controller's instruction.	We have inquired about documentation for the processing being consistent with the controller's instruction, and we have inspected documentation for this.	No significant deviations noted.
A.3	The processor immediately notifies the controller if an instruction according to the processor's opinion 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 documentation for the company notifying the controller if an instruction is contrary to current legislation, and we have inspected documentation for this.	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. Regularly – and at least annually – an assessment is made of whether the procedures should be updated.	We have inquired about documentation for the company's established security measures for the processing of personal data being consistent with the agreed measures, and we have inspected processor agreements and information security policy. Additionally, we have inquired about documentation for ongoing periodic control of the information security policy, and we have inspected the control.	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 documentation for the company having prepared a risk analysis of the processing of personal data, and we have inspected the risk analysis. Additionally, we have inquired about documentation for ongoing updating of the risk analysis, and we have inspected documentation for this.	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 documentation for local media having installed antivirus, and we have inspected documentation for this. Additionally, we have inquired about documentation for servers having installed antivirus, and we have inspected assurance report from sub-supplier.	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 documentation for access to servers being protected by firewall, and we have inspected assurance report from sub-supplier.	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 assurance report from sub-supplier as well as documentation for segregation of customer databases.	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 documentation for access to the solution and servers that process personal data occurring according to a work-related need, and we have inspected documentation for access to personal data occurring according to a work-related need.	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. The monitoring comprises: • Notification of potential changes or events that may influence security or system access	We have inquired about documentation for the processor having established monitoring with alarming for systems and databases, and we have inspected assurance report from supplier.	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 documentation for the encryption of personal data, and we have inspected documentation for encryption of SSL for speedadmin.dk.	No significant deviations noted.

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 events, including:
	  ○ Changes to log settings, including deactivation of logging
	  ○ Changes to users' system rights
		We have inquired about documentation for logging on systems, networks, and databases, and we have inspected documentation for this.
		Additionally, we have inquired about documentation for sub-supplier having established logging of systems, databases, and networks, and we have inspected assurance report from sub-supplier.
			No significant deviations noted.

B.10	Personal data used for development, test or similar are always pseudonymised or anonymised. Use solely occurs in order to meet the responsible party's purpose as agreed, and on behalf of this party.	We have inquired about documentation for segregation of production and test data, and we have inspected documentation for this.	No significant deviations noted.

No.	Processor's control activity	Auditor's performed test	Test result
B.11	The established technical measures are periodically tested by means of vulnerability scans and penetration tests.	We have inquired about documentation for periodic vulnerability scans and penetration tests, and we have inspected assurance report from sub-supplier.	No significant 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 documentation for changes to databases, systems, and networks following specific procedures, and we have inspected assurance report from sub-supplier of servers.	No significant deviations noted.
B.13	There is a formalised procedure for allocation and removal of user access to personal data. Users' access is regularly reviewed, including that rights continuously can be founded on a work-related need.	We have inquired about documentation for access management, and we have inspected documentation for this. Additionally, we have inquired about documentation for ongoing review of user access, and we have inspected the periodic control. Furthermore, we have inquired about and have inspected assurance report from sub-supplier.	No significant deviations noted.
B.14	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 about documentation for the establishment of physical access security at the operations supplier, and we have inspected assurance report from supplier. Additionally, we have inquired about documentation for the company having an overview of key fobs, and we have inspected the overview.	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 ongoing updating of the information security policy, and we have inspected control for periodic update of the information security policy. Additionally, we have inquired about documentation for information security policies being communicated to controllers.	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 entered processor agreements, and we have inspected the control of the policy.	No significant deviations noted.
C.3	The processor's employees are checked in connection with employment. This check comprises the following, to the relevant degree: • References from prior employment • Criminal record • Certificates and diplomas	We have inquired about documentation for the processor obtaining references or similar in connection with employment, and we have inspected the procedure.	No significant deviations noted.
C.4	At employment, employees sign a confidentiality agreement. In addition, the employee is introduced to the information security policy 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 documentation for employees signing a confidentiality agreement in connection with employment, and we have inspected documentation for this. Additionally, we have inquired about documentation for the employee being informed of information security in the company, and we have inspected documentation for this.	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 documentation for the company performing access management, and we have inspected documentation for the creation and deletion of users as well as allocation of rights. Additionally, we have inquired about ongoing access control, and we have inspected an access control. Furthermore, we have inquired about documentation for the company maintaining an overview of supplied keys, and we have inspected documentation for this.	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 documentation for the company regularly training employees, and we have inspected the procedure for employee security.	No significant deviations noted.
C.8	The processor has considered the need for a DPO, and has ensured that the DPO has adequate professional capability to perform their duties.	We have inquired about documentation for the company having a DPO with adequate professional capability, and we have inspected documentation for the DPO having adequate professional capability.	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. Regularly – and at least annually – an assessment is made of whether the procedures should be updated.	We have inquired about documentation for the company, following the termination of the agreement, deleting or returning personal data according to the requirements in processor agreements, and we have inspected processor agreements and policies. Additionally, we have inquired about ongoing updating of the above, and we have inspected documentation for this.	No significant deviations noted.
D.2	The following specific requirements to the processor's storage period and deletion routines have been agreed: • Must be deleted or returned to the controller according to instruction	We have inquired about documentation for requirements to the processor's storage periods and deletion routines, and we have inspected processor agreements.	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 documentation for the processor either returning or deleting personal data at the termination of the agreement, and we have inspected processor agreements and policies for instruction on deletion or return.	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. Regularly – and at least annually – an assessment is made of whether the procedures should be updated.	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 processing locations, 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. Regularly – and at least annually – an assessment is made of whether the procedures should be updated.	We have inquired about documentation for the company having a procedure for supplier management, and we have inspected the procedure. Additionally, we have inquired about ongoing updating of the procedure, and we have inspected documentation for this. Furthermore, we have inquired about documentation for inspection of sub-processors who do not have assurance reports, and we have inspected the control. We have inquired about documentation for the company having entered processor agreements containing requirements to the processor at the use of sub-processors, including requirements on sub-processor agreements and instruction, and we have inspected an example of a processor agreement and sub-processor agreements.	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 the processing of personal data that is 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 documentation for the company informing the controller in case of changes to the use of specifically approved sub-processors, and that this is approved by the controller, and we have inspected documentation for this.	We have noted that the company has not communicated changes to sub-processors to the controllers within the set time limit. However, we have noted that the company subsequently has sent notification to the controllers. 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 obligations 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, including: • Name • Description of the processing	We have inquired about documentation for approved sub-processors being listed with adequate identification, and we have inspected the agreements.	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. The controller is informed of the follow-up being performed at the sub-processor.	We have inquired about documentation for the company regularly performing control of each sub-processor, and we have inspected documentation for this.	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. Regularly – and at least annually – an assessment is made of whether the procedures should be updated.	We have inquired about documentation for whether the company transfers personal data to third countries, and we have inspected processor agreements with sub-processors.	No significant deviations noted.
G.2	The processor may only transfer personal data to third countries or international organisations according to instruction from the controller.	Not applicable, as processor does not perform transfer of personal data to third countries in relation to the scope of this assurance report.	No significant deviations noted.
G.3	In connection with transfer of personal data to third countries or international organisations the processor has assessed and documented that a valid ground for transfer exists.	Not applicable, as processor does not perform transfer of personal data to third countries in relation to the scope of this assurance report.	No 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 documentation for the company being able to assist the controller with personal data requests, and we have inspected the procedure. Additionally, we have inquired about ongoing updating of the procedure, and we have inspected documentation for this. Furthermore, we have inspected documentation for users being able to be anonymised, and we have inspected documentation for this. We have also inquired about documentation for tickets containing personal data being deleted, and we have inspected the documentation. We have inquired about documentation for ongoing control of the technical measures, including deletion of relevant tickets, and we have inspected documentation for this.	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 a technical example of handing over/insight into data as well as deletion of users, and we have inspected documentation for this.	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 controllers 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 the company having a procedure for the management of security incidents, and we have inspected documentation for this. Additionally, we have inquired about documentation for periodic review and updating of the procedure, and we have inspected documentation for this.	No significant deviations noted.
I.2	The processor has established the following controls for identification of any personal data breaches: • Employee awareness • Monitoring network traffic	We have inquired about documentation for the controller regularly performing the following: • Employee awareness • Monitoring network traffic Additionally, we have inspected documentation for this.	No significant deviations noted.
I.3	In case of a personal data breach the processor has informed the controller without undue delay and no later than 48 hours after finding out that the personal data breach has occurred at the processor or a sub-processor.	We have inquired about documentation for the company communicating personal data breaches without undue delay to relevant controllers, and we have inspected the procedure for personal data breaches as well as the log of security incidents.	It has not been possible for us to test the procedure for managing personal data breaches, as the company has not had any security incidents following the commencement of the procedure. No further 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 documentation for the company as a minimum providing the controller with the following information in relation to personal data breaches: • Description of the type of personal data breach • Description of probable consequences of the personal data breach • Description of measures taken or suggested taken in order to manage the personal data breach We have inspected documentation for the above-mentioned. Additionally, we have inquired about whether the company maintains a log of personal data breaches, and we have inspected documentation for this. Furthermore, we have inspected documentation for regular review of information security incidents, and we have inspected documentation for this.	No significant 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 wherein it is ensured that the data subject has received contact information on the controller, information on the purpose of the processing of the personal data as well as other information necessary for fulfilling the duty of disclosure.

No.	Processor's control activity	Auditor's performed test	Test result
J.1	Written procedures are in place for obtaining written consent for the processing of personal data. Regularly – and at least annually – an assessment is made of whether the procedures should be updated.	We have inquired about documentation for the company technically being able to support consent and the duty of disclosure, and we have inspected documentation for this.	No significant deviations noted.
J.2	Technical measures have been implemented that ensure that it can be documented what information has been given when providing the consent.	We have inquired about documentation showing that the company can document that consent has been given, and we have inspected documentation for this.	Not applicable, as the company does not gather consent on behalf of the controller.
J.3	Written procedures are in place in which is described how it is ensured that the data subject receives information about the purpose of processing of personal data as well as information on any transfer of personal data to recipients, third countries, or international organisations, or how the processor can assist the controller with this. Regularly – and at least annually – an assessment is made of whether the procedures should be updated.	Not applicable, as the company is not responsible for the duty of disclosure.	Not applicable, as the company is not responsible for the duty of disclosure.
J.4	Regularly – and at least annually – a control is performed for all data subjects having received the description of the data subject's right to insight, correction, or erasure of personal data.	Not applicable, as the company is not responsible for the duty of disclosure.	Not applicable, as the company is not responsible for the duty of disclosure.

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 documentation for the company having prepared a record of processing activities, 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 documentation for the company regularly assessing and updating the record, and we have inspected documentation for this.	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 inspected documentation for the management having ensured that the record of categories of processing activities for each controller is adequate, updated, and correct.	No significant deviations noted.