Assurance report

SpeedAdmin ApS

Independent auditor's ISAE 3000 type 1 assurance report on information security and measures pursuant to the data processing agreement with customers using SpeedAdmin for schools of music and culture as per 27 April 2026

June 2026

Grant Thornton | www.grantthornton.dk
Lautrupsgade 11, 2100 København Ø
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Table of contents

Section 1: SpeedAdmin ApS' statement

The accompanying description has been prepared for customers who have signed a data processing agreement with SpeedAdmin ApS and who have a sufficient understanding to consider the description along with other information, including information about controls, which the data controller himself has performed, in assessing whether the requirements in EU's regulation on protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter the General Data Protection Regulation) have been complied with.

SpeedAdmin ApS uses the following sub-processors: Zendesk Inc., Unit IT A/S, Link Mobility A/S and Microsoft Ireland Ltd. This report does not include control objectives and affiliated controls with SpeedAdmin ApS' sub-processors. Certain control objectives in the description can only be achieved, if the sub-processor's controls, assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities, performed by sub-processors.

Some of the control objectives stated in SpeedAdmin ApS' description in Section 3 of SpeedAdmin for schools of music and culture can only be achieved if the complementary user entity controls with the data controllers are appropriately designed and works effectively with the controls with SpeedAdmin ApS. This report does not include the appropriateness of the design and the operating effectiveness of these complementary user entity controls.

SpeedAdmin ApS confirms that:

a) The accompanying description, Section 3, fairly presents SpeedAdmin for schools of music and culture which has processed personal data for data controllers subject to the Regulation as per 27 April 2026. The criteria used in making this statement were that the accompanying description:

   (i) Presents how SpeedAdmin for schools of music and culture was designed and implemented, including:

   - The types of services provided, including the type of personal data processed
   - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete, and restrict processing of personal data
   - The procedures used to ensure that data processing has taken place in accordance with contract, instructions, or agreement with the data controller
   - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality
   - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation
   - The procedures supporting in the event of breach of personal data security that the data controller may report this to the supervisory authority and inform the data subjects
   - The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed
   - Controls that we, in reference to the scope of SpeedAdmin ApS have assumed would be implemented by the data controllers and which, if necessary, in order to achieve the control objectives stated in the description, are identified in the description
   - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data

(ii) Does not omit or distort information relevant to the scope of SpeedAdmin for schools of music and culture being described for the processing of personal data while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of SpeedAdmin for schools of music and culture that the individual data controllers might consider important in their particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were, in our view, suitably designed and implemented as per 27 April 2026, if relevant controls with sub-processors were operationally effective and data controller has performed the complementary user entity controls, assumed in the design of SpeedAdmin ApS' controls as per 27 April 2026.

The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified; and

(ii) The identified controls would, if implemented as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

c) Appropriate technical and organisational safeguards were established and maintained to comply with the agreements with the data controllers, sound data processing practices and relevant requirements for data processors in accordance with the Regulation.

Sønderborg, 22 June 2026
SpeedAdmin ApS

Michael Jørgen Hamann
Chief Executive Officer

Section 2: Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to SpeedAdmin ApS' data processing agreement with data controllers

To: SpeedAdmin ApS, their customers, and their auditors

Scope

We were engaged to provide assurance about a) SpeedAdmin ApS' description, Section 3, of SpeedAdmin for schools of music and culture in accordance with the data processing agreement with costumers as per 27 April 2026 and about b) the design and implementation of controls related to the control objectives stated in the Description.

SpeedAdmin ApS uses the following sub-processors: Zendesk Inc., Unit IT A/S, Link Mobility A/S and Microsoft Ireland Ltd. This statement does not include control objectives and related controls at SpeedAdmin ApS' sub-processors. Certain control objectives in the description can only be achieved if the sub-processor's controls, assumed in the design of our controls, are appropriately designed, and operating effectively. The description does not include control activities performed by sub-processors.

Some of the control objectives stated in SpeedAdmin ApS' description in Section 3 of SpeedAdmin for schools of music and culture, can only be achieved if the complementary user entity controls with the data controller have been appropriately designed and operating effectively with the controls with SpeedAdmin ApS. The report does not include the appropriateness of the design and operational effectiveness of these complementary user entity controls.

Our opinion is based on reasonable assurance.

SpeedAdmin ApS' responsibilities

SpeedAdmin ApS is responsible for: preparing the Description and the accompanying statement, Section 1, including the completeness, accuracy, and the method of presentation of the Description and statement, providing the services covered by the Description; stating the control objectives; and designing and implementing controls to achieve the stated control objectives.

Grant Thornton's independence and quality control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour and ethical requirements applicable to Denmark. Grant Thornton applies International Standard on Quality Management 1, ISQM 1, requiring that we maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on SpeedAdmin ApS' Description and on the design and implementation of controls related to the control objectives stated in that Description, based on our procedures.

We conducted our engagement in accordance with International Standard on Assurance Engagements 3000, "Assurance Engagements Other than Audits or Reviews of Historical Financial Information", and additional requirements under Danish audit regulation, to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are appropriately designed and implemented.

An assurance engagement to report on the Description, design, and implementation of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of its SpeedAdmin for schools of music and culture and about the design and implementation of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not appropriately designed. Our procedures included testing the implementation of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved.

An assurance engagement of this type also includes evaluating the overall presentation of the Description, the appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data processor and described in Section 1.

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

Limitations of controls at a data processor

SpeedAdmin ApS' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of SpeedAdmin for schools of music and culture that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect personal data breaches. Furthermore, the projection of any evaluation of the operating effectiveness to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the Management's statement Section 1.

In our opinion, in all material respects:

(a) the description fairly presents how SpeedAdmin for schools of music and culture were designed and implemented as per 27 April 2026.

(b) the controls related to the control objectives stated in the description were suitably designed and implemented as per 27 April 2026

Description of tests of controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section 4.

Intended users and purpose

This report and the description of tests of controls in Section 4 are intended only for data controllers who have used SpeedAdmin ApS' SpeedAdmin for schools of music and culture who have a sufficient understanding to consider it along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the Regulation have been complied with.

Sønderborg, 22 June 2026

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Martin Brogaard Nielsen
Partner, CISA, CIPP/E, CRISC

Section 3: SpeedAdmin ApS' description of processing activity for the supply of SpeedAdmin for schools of music and culture

System description

The purpose of the data processor's processing of personal data on behalf of the data controller is to provide the SpeedAdmin Play! administration system to music and culture schools.

It is the music and culture schools that are responsible for providing the data they require in order to carry out their day-to-day administrative tasks in SpeedAdmin Play! This makes the music and culture schools the data controllers in relation to the data subjects in the system.

The processing of personal data is in accordance with the main agreement (licence agreement) between SpeedAdmin ApS and the music and culture schools, as well as the data processing agreement entered into at the start of the service provision.

The system is 100% web-based, so there is no need to install or download any software onto the computer you are using. However, it is possible to download the SpeedAdmin Play! app onto smartphones and tablets, which can be used by teachers, students and guardians alike.

Nature of the processing

The data processor's processing of personal data on behalf of the data controller is carried out exclusively in accordance with the data controller's instructions. The data processor does not use the personal data for any purposes other than those described in the data controller's instructions.

Personal data

- CPR number (DK) and personal identification number (NO and SE)
- Date of birth (UK and DE)
- Address, postcode
- Full name
- Email
- Mobile and telephone number

Categories of data subjects covered by the data processing agreement:

- Staff at music and culture schools
- Pupils
- Guardians
- Any contact persons at the music and culture school's partners

Practical measures

The management at SpeedAdmin has approved all measures, internal standards and the various annual audits carried out internally at SpeedAdmin Play!

All SpeedAdmin employees have been briefed on personal data and information security. Annual internal security awareness training is held for all employees, during which internal standards are reviewed, along with information relating to the GDPR and IT security. All standards are available to all employees. In the event of major changes to the standards, all employees are informed accordingly.

The system generates automatic logs. Among other things, all logins to the system are logged, including failed logins. Changes made to pupils, guardians and teachers are logged. In addition, person-specific searches within the system are also logged.

Developments in the system that may affect the rights of data subjects are recorded in a log, and SpeedAdmin's DPO is involved in the process. Any security breaches are recorded, along with how they are handled. This log will be reviewed annually, with a focus on how the security breaches have been handled.

Risk assessment

SpeedAdmin ApS has conducted a risk assessment of potential threats to the system and data security. These threats have been evaluated based on the likelihood of occurrence and the potential impact should they materialise.

This risk assessment is reviewed at least once a year. As part of this review, particular attention is given to whether any new threats have emerged since the previous assessment. In addition, the risk assessment is updated if measures have been implemented or if new proposed solutions have been identified.

Any changes to the risk assessment will always be approved and signed off by one of SpeedAdmin ApS' managers.

Control measures

Processing activities – instructions
In our data processing agreements with our customers, the customers' instructions regarding data processing are clearly defined. These instructions are the only basis on which we process data.

Should a customer require further information regarding the processing of their data, we are available to provide it. Any such request is handled as quickly as possible upon receipt.

Customers have the option to create consent declarations for users, which must be accepted when signing up for a subject or course. This includes, among other things, GDPR consent, which all our customers use. In addition, customers may also design their own consents, for example relating to the use of photos, videos, etc.

We maintain an internal procedure for handling unlawful instructions should we receive any from a customer. All employees are familiar with this procedure and are therefore able to act appropriately if they receive an unlawful instruction.

We also maintain an Article 30 record of processing activities covering the various types of personal data processing we carry out, both as a data processor (on behalf of our customers) and as a data controller (in relation to our subcontractors). This record is also available to employees so they can consult it when needed.

The Article 30 record is reviewed and revised at least once a year at the beginning of each new year, or continuously as required. Reminders have been set up for the responsible parties to ensure that these revisions are carried out.

In addition to the Article 30 record, we also manage all employee user access rights. We maintain an overview of all employee access permissions and update it whenever changes occur.

Procedure controls
Once a year, or as needed, all internal procedures are reviewed. In addition, various records and logs are also examined and revised. This allows us to maintain an overview of the overall handling of cases and assess whether any procedures need to be adjusted or updated.

All employees have automatic email deletion enabled in Outlook. Emails older than two years are automatically deleted.

Procedure review
As previously mentioned, all employee procedures are reviewed annually during our Security Awareness Training Day. It is important that all employees are informed of and familiar with these procedures so that everyone is able to act appropriately, for example when receiving an enquiry from a customer.

These procedures are revised as needed and at least once a year.

Procedures – access management
SpeedAdmin's management is responsible for deciding and administering which access rights individual employees are granted.

All access rights are recorded in a document. This document is updated whenever any changes are made in relation to access permissions.

Personal passwords are required both for employees' computers and for the system itself.

The majority of SpeedAdmin employees have access to the office in Sønderborg. They are issued with a key and a key fob, both of which are marked with an identification number that is recorded in the access management document for each employee.

When an employee leaves the company, the relevant internal procedure must be followed regarding the return of keys and key fobs, as well as the termination of all access rights held by that individual.

Within the system itself, user permission groups are in place. This means that not all users have the same rights within the system, as each permission group defines which functions are available to the individual user.

In addition to permission groups within the system, all actions carried out in the system are logged, including who performed each action.

Procedures – risk management
SpeedAdmin has prepared a risk assessment based on the potential risks and threats that may affect SpeedAdmin Play! This assessment is revised as needed, but at least once a year.

For risks assessed as high (minimum level 10), measures are developed to prevent the risk from materialising wherever possible. If this is not possible, measures are instead implemented to mitigate the consequences should the risk materialise.

Procedures – development
The internal procedure governing the development of new or existing features that may affect data subjects' rights and/or personal data must be followed.

Under this procedure, the developers responsible for the specific development task must ensure that the development process is recorded in an internal log.

In addition to maintaining this log, the DPO must also be involved before the development is deployed to the system. The DPO's role is to help ensure that data subjects within the system are protected in the best possible way and in accordance with the General Data Protection Regulation (GDPR).

Procedures – handling of personal data requests
SpeedAdmin does not process personal data requests submitted directly by data subjects. As we act solely as a data processor rather than a data controller, we must not and do not handle such requests. It is the data controllers, our customers, who are responsible for processing personal data requests.

It is therefore rare that we would receive such requests directly. However, as this cannot be entirely ruled out, this scenario is addressed in our internal procedure concerning data subjects' rights.

If we receive a personal data request from a data subject, we refer the individual to contact the relevant affiliated school. In addition, all such requests are recorded in a log, which is reviewed as needed or at least once a year in order to maintain oversight and assess whether any updates to the procedure are necessary.

Procedures – security incidents
SpeedAdmin ApS logs security incidents in accordance with the internal procedure on data breaches. It is important that the DPO is involved as soon as a security incident or breach is identified.

In the event of a security breach, the handling of the incident must be recorded in an internal log. This log must be continuously updated from the point of detection until the case is fully resolved.

The log is reviewed once a year. During this review, the handling of incidents from the past year is assessed, with a particular focus on how the incidents were managed and whether any adjustments to the procedure are required. If the procedure is updated, all employees are informed accordingly.

If a customer inadvertently includes sensitive personal data via our support system, SpeedAdmin staff will inform the customer that they must use the ID numbers assigned to each user in SpeedAdmin Play! instead.

In addition, it is possible to mark a security breach or incident as such within our support system. It is then also possible to delete the ticket if it contains personal data. When customers use the "contact support" function within the system, it is ensured that no personal data is included in screenshots, as these are automatically blurred.

Sub-processors
We have chosen to use sub-processors as we believe they contribute to providing the best overall solution for all our customers.

Sub-processors must at all times have appropriate safeguards in place against unlawful electronic or physical intrusion, vandalism, theft, hacking, computer viruses, denial-of-service attacks, and other similar security breaches. They must also ensure protection against risks such as fire, storms, water damage, and other conditions that may jeopardise SpeedAdmin's ability to fulfil its contractual obligations.

An annual review is carried out of all sub-processors. We obtain IT audit statements or similar documentation from sub-processors where such reports are available. If no such documentation exists, we issue an annual questionnaire covering their procedures and measures for ensuring a high level of IT security.

All non-confidential material related to our review process may, upon request from the data controller, be provided to the data controller.

Third countries
It has been decided internally that SpeedAdmin neither stores nor transfers data to third countries. This is therefore always a factor that is assessed before SpeedAdmin decides to engage any new sub-processor.

Although SpeedAdmin's sub-processors do not store data in third countries, some sub-processors may still have roots or parent companies located in third countries. As a result, SpeedAdmin has taken precautions to ensure that any relevant sub-processors have a valid legal basis for data transfers in the event of any potential transfer of personal data.

We have assessed whether Binding Corporate Rules (BCR) and Standard Contractual Clauses (SCCs) are in place, and we have prepared a Transfer Impact Assessment (TIA) for the affected sub-processors.

Employees
When an employee is hired, the IT security policy and the internal procedures are reviewed with them. In addition, an employee declaration must be signed, which is also included as an appendix to our IT security policy.

Upon termination of employment, the relevant procedure for employee offboarding is followed.

Complementary user entity controls

- The data controllers are responsible for deleting logs themselves.
- Only super users are permitted to anonymise users in the system.
- If the data controller downloads Excel spreadsheets from SpeedAdmin Play!, they are responsible for ensuring that these are subsequently deleted.
- The data controllers must be aware of emails sent from the system regarding locked users.
- The data controllers have their own obligation to provide information to the data subjects in SpeedAdmin Play! We naturally assist by providing information regarding the processing activities.

Section 4: Control objectives, controls, tests, and results hereof

We conducted our engagement in accordance with ISAE 3000, assurance engagements other than audits or review of historical financial information.

Our test of the implementation has included the control objectives and attached controls, selected by management and which are stated in the control objectives A-I below. Our test has included the controls; we find necessary to establish reasonable assurance for compliance with the articles stated as per 27 April 2026.

Our statement, does not apply to controls, performed at SpeedAdmin ApS' sub-processors.

Further, controls performed at the data controller are not included in this statement.

We performed our test of controls at SpeedAdmin ApS by the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at SpeedAdmin ApS. The interviews have included questions about, how controls are performed.
Observation	Observing how controls are performed.
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 effective when implemented. Further, it is assessed whether controls are monitored and controlled adequately and with suitable intervals.
Re-performance	Re-performance of controls to verify that the control is working as assumed.

List of control objectives compared to GDPR-articles, ISO 27701, and ISO 27001/2

Below, control objectives are mapped against the articles in GDPR, ISO 27701 and ISO 270001/2. Articles and points about main areas are written in bold.

Control activity	GDPR articles	ISO 27701	ISO 27001/2:2013
A.1	5, 26, **28**, 29, 30, 32, 40, 41, 42, 48	8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, **8.2.2**	*New scope compared to ISO 27001/2*
A.2	**28**, 29, 48	8.5.5, 6.15.2.2, **6.15.2.2**	18.2.2
A.3	**28**	**8.2.4, 6.15.2.2**	18.2.2
B.1	31, **32**, 35, 36	**5.2.2**	4.2
B.2	**32,** 35, 36	**7.2.5, 5.4.1.2, 5.6.2**	6.1.2, 5.1, 8.2
B.3	**32**	**6.9.2.1**	**12.2.1**
B.4	28 stk. 3; litra e, **32; stk. 1**	**6.10.1.1, 6.10.1.2, 6.10.1.3**, 6.11.1.3	**13.1.2**, 13.1.3, 14.1.3, 14.2.1
B.5	32	6.6.1.2, 6.10.1.3	9.1.2, 13.1.3, 14.2.1
B.6	**32**	**6.6**	9.1.1, 9.2.5
B.7	**32**	**6.9.4**	12.4
B.8	**32**	**6.15.1.5**	18.1.5
B.9	**32**	**6.9.4**	12.4
B.10	**32**	**6.11.3**	14.3.1
B.11	**32**	**6.9.6.1**	12.6.1
B.12	28, **32**	**6.9.1.2, 8.4**	12.1.2
B.13	**32**	**6.6**	9.1.1
B.14	**32**	**7.4.9**	*New scope compared to ISO 27001/2*
B.15	**32**	**6.8**	11.1.1-6
C.1	**24**	**6.2**	5.1.1, 5.1.2
C.2	**32, 39**	**6.4.2.2, 6.15.2.1, 6.15.2.2**	7.2.2, 18.2.1,18.2.2
C.3	**39**	**6.4.1.1-2**	7.1.1-2
C.4	28, 30, **32, 39**	**6.10.2.3**, 6.15.1.1, 6.4.1.2	7.1.2, 13.2.3
C.5	**32**	**6.4.3.1, 6.8.2.5, 6.6.2.1**	7.3.1, 11.2.5, 8.3.1
C.6	**28,** 38	**6.4.3.1, 6.10.2.4**	7,3.1, 13.2.4
C.7	**32**	**5.5.3, 6.4.2.2**	7.2.2, 7.3
C.8	**38**	**6.3.1.1, 7.3.2**	6.1.1
C.9	6, 8, 9, 10, 15, 17, 18, 21, 28, **30**, 32, 44, 45, 46, 47, 48, 49	6.12.1.2, 6.15.1.1, 7.2.2, **7.2.8**, 7.5.1, 7.5.2, 7.5.3, 7.5.4, **8.2.6**, 8.4.2, 8.5.2, 8.5.6	*New scope compared to ISO 27001/2*
D.1	6, 11, **13, 14,** 32	**7.4.5**, **7.4.7**, 7.4.4	*New scope compared to ISO 27001/2*
D.2	6, 11, 13, 14, **32**	**7.4.5**, **7.4.7**, 7.4.4	*New scope compared to ISO 27001/2*
D.3	13, **14**	**7.4.7**, 7.4.4	*New scope compared to ISO 27001/2*
E.1	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*New scope compared to ISO 27001/2*
E.2	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*New scope compared to ISO 27001/2*
F.1	6, 8, 9, 10, 17, 18, 22, 24, 25, 28, **32,** 35, 40, 41, 42	5.2.1, **7.2.2**, **7.2.6**, 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7	15
F.2	**28**	**8.5.7**	15
F.3	**28**	**8.5.8**, 8.5.7	15
F.4	**33, 34**	**6.12.1.2**	15
F.5	**28**	**8.5.7**	15
F.6	**33, 34**	**6.12.2**	15.2.1-2
G.1	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, **8.5.1**, 8.5.2, 8.5.3	13.2.1, 13.2.2
G.2	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1,** 7.5.2, 7.5.3, 7.5.4, **8.4.2,** 8.5.2, 8.5.3	13.2.1
G.3	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
H.1	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*New scope compared to ISO 27001/2*
H.2	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*New scope compared to ISO 27001/2*
I.1	**33, 34**	**6.13.1.1**	16.1.1-5
I.2	**33, 34**, 39	6.4.2.2, **6.13.1.5, 6.13.1.6**	16.1.5-6
I.3	**33, 34**	**6.13.1.4**	16.1.5
I.4	**33, 34**	**6.13.1.4,** 6.13.1.6	16.1.7

Control objective A - Instructions regarding processing of personal data

Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistently with the data processing agreement entered into.

No.	*SpeedAdmin ApS' control activity*	*Tests performed by Grant Thornton*	*Result of test*
A.1	Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist to ensure that personal data are only processed according to instructions. We have inspected that procedures are up to date.	No deviations noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	We have inspected that management ensures that personal data are only processed according to instructions. We have inspected that a sample of personal data processing operations are conducted consistently with instructions.	No deviations noted.
A.3	The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions.	We have inspected that procedures are in place for informing the data controller of cases where the processing of personal data is evaluated to be against legislation. We have inquired whether the data processor has received instructions within the last six months, which, in the data processor's opinion, contravene the data protection regulation or data protection provisions in other EU law or the national law of the member states.	We have been informed that the data processor has not received instructions that, in the opinion of the data processor, are in conflict with the General Data Protection Regulation or data protection provisions in other EU or Member States' national law within the last six months. No deviations noted.

Control objective B - Technical measures

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	*SpeedAdmin ApS' control activity*	*Tests performed by Grant Thornton*	*Result of test*
B.1	Written procedures exist which include a requirement that safeguards agreed are established for the processing of personal data in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist to ensure establishment of the safeguards agreed. We have inspected that procedures are up to date. We have, by sample test, inspected that the safeguards agreed in data processing agreements have been established.	No deviations noted.
B.2	The data processor has performed a risk assessment and based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the safeguards agreed with the data controller.	We have inspected that the risk assessment performed is up to date and comprises the current processing of personal data.	No deviations noted.
B.3	For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.	We have inspected that, for the systems and databases used in the processing of personal data, antivirus software has been installed. We have inspected that antivirus software is up to date.	No deviations noted.
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	We have inspected that external access to systems and databases used in the processing of personal data takes place only through a secured firewall. We have inspected that the firewall has been configured in accordance with the relevant internal policy.	No deviations noted.
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	We have inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. We have inspected network diagrams and other network documentation to ensure appropriate segmentation.	No deviations noted.

Control objective B - Technical measures

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	*SpeedAdmin ApS' control activity*	*Tests performed by Grant Thornton*	*Result of test*
B.6	Access to personal data is isolated to users with a work-related need for such access.	We have inspected that formalised procedures are in place for restricting users' access to personal data. We have inspected that formalised procedures are in place for following up on users' access to personal data being consistent with their work-related need. We have inspected that access is restricted to the employees' work-related need for a sample of users' access to systems and databases.	No deviations noted.
B.7	For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.	We have inspected that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. We have, by sample test, inspected that alarms were followed up on.	No deviations noted.
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	We have inspected that formalised procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognised algorithm. We have, by sample test, inspected that transmission of personal data is done in accordance with internal policy for encryption.	No deviations noted.
B.9	Logging has been established in systems, databases, and networks. Log data are protected against manipulation, technical errors and are reviewed regularly.	We have inspected that formalised procedures exist for setting up logging of user activities. We have, by sample test, inspected that logging is in compliance with the procedure. We have inspected that user activity data collected in logs are protected against manipulation or deletion.	No deviations noted.

Control objective B - Technical measures

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	*SpeedAdmin ApS' control activity*	*Tests performed by Grant Thornton*	*Result of test*
B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.	We have inspected that formalised procedures exist for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised form. We have, by sample test, inspected that personal data included in development or test databases are pseudonymised or anonymised.	No deviations noted.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	We have inspected that formalised procedures exist for regularly testing technical measures, including for performing vulnerability scans and penetration tests. We have, by sample test, inspected that documentation exists regarding regular testing of the established technical measures. We have inspected that any deviations or weaknesses in the technical measures have been responded to in a timely and satisfactory manner.	No deviations noted.
B.12	Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches.	We have inspected that formalised procedures exist for handling changes to systems, databases, or networks, including handling of relevant updates, patches, and security patches. We have inspected that the latest implemented change to systems, databases and networks has been handled according to the procedure for this.	No deviations noted.
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	We have inspected that formalised procedures exist for granting and removing users' access to systems and databases using to process personal data. We have inspected that documentation exists that user accesses granted are evaluated and authorised on a regular basis – and at least once a year.	No deviations noted.

Control objective B - Technical measures

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	*SpeedAdmin ApS' control activity*	*Tests performed by Grant Thornton*	*Result of test*
B.14	Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication.	We have inspected that formalised procedures exist to ensure that two-factor authentication is applied in the processing of personal data that involves a high risk for the data subjects. We have inspected documentation that access to personal data is done by using two-factor authentication.	No deviations noted.
B.15	Physical access safeguards have been established so as to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed.	We have inspected documentation that the data processor has a list of keys to the office.	No deviations noted.

Control objective C - Organisational measures

Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

No.	*SpeedAdmin ApS' control activity*	*Test performed by Grant Thornton*	*Result of test*
C.1	Management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The IT security policy is based on the risk assessment performed. Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.	We have inspected that an information security policy exists that Management has considered and approved within the past year. We have inspected documentation that the information security policy has been communicated to the data processor's employees.	No deviations noted.
C.2	Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.	We have, by sample test, inspected that the requirements in data processing agreements are covered by the requirements of the information security policy for safeguards and security of processing.	No deviations noted.
C.3	The employees of the data processor are screened as part of the employment process.	We have inspected that formalised procedures are in place to ensure screening of the data processor's employees as part of the employment process. We have, by sample testing, inspected that screening of newly hired employees has been performed in accordance with the procedure.	No deviations noted.
C.4	Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.	We have inspected that employees appointed have signed a confidentiality agreement. We have, by sample test, inspected that new employees have been introduced to relevant procedures and policies.	No deviations noted.

Control objective C - Organisational measures

Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

No.	*SpeedAdmin ApS' control activity*	*Test performed by Grant Thornton*	*Result of test*
C.5	For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned.	We have inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal and that assets such as access cards, computers, mobile phones, etc. are returned. We have inspected that rights have been deactivated or terminated, and that assets have been returned for the most recently resigned employee.	No deviations noted.
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	We have inspected that formalised procedures exist to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality. We have inspected that there is documentation for maintaining the confidentiality agreement and general confidentiality has been communicated for the most recently resigned employee.	No deviations noted.
C.7	Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data.	We have inspected that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data. We have inspected documentation that all employees who have either access to or process personal data have completed the awareness training provided.	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 inspected the assessment of the need for a DPO and ensured that the company has assessed the need for a DPO. We have inspected documentation that the DPO has been involved in relevant tasks.	No deviations noted.

Control objective C - Organisational measures

Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

No.	*SpeedAdmin ApS' control activity*	*Test performed by Grant Thornton*	*Result of test*
C.9	The processor keeps a record of categories of processing activities for each data controller. 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 that the categories of processing activities have been updated and approved by management. We have inspected that records of processing activities have been updated and approved by management.	No deviations noted.

Control objective D - Return and deletion of personal data

Procedures and controls are complied with to ensure that personal data are deleted or returned if arrangements are made with the data controller to this effect.

No.	*SpeedAdmin ApS' control activity*	*Grant Thornton's test*	*Result of test*
D.1	Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller. We have inspected that the procedures are up to date.	No deviations noted.
D.2	Specific requirements have been agreed with respect to the data processor's storage periods and deletion routines.	We have inspected that the existing procedures for storage and deletion, include specific requirements for the data processor's storage periods and deletion routines. We have, by sample test, inspected that documentation exists of personal data being stored in accordance with the agreed storage periods in the data processing agreements.	No deviations noted.

Control objective D - Return and deletion of personal data

Procedures and controls are complied with to ensure that personal data are deleted or returned if arrangements are made with the data controller to this effect.

No.	*SpeedAdmin ApS' control activity*	*Grant Thornton's test*	*Result of test*
D.3	Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been: • Returned to the data controller; and/or • Deleted if this is not in conflict with other legislation.	We have inspected that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data. For most of the terminated data processing agreements inspected, we have verified that the agreed deletion or return of data has taken place. We have inspected that there is documentation that the agreed deletion or return of data has been carried out for the most recently terminated data processing.	No deviations noted.

Control objective E – Storage of personal data

Procedures and controls are complied with to ensure that the data processor will only store personal data in accordance with the agreement with the data controller.

No.	*SpeedAdmin ApS' control activity*	*Test performed by Grant Thornton*	*Result of test*
E.1	Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements. We have inspected that the procedures are up to date.	No deviations noted.

Control objective E – Storage of personal data

Procedures and controls are complied with to ensure that the data processor will only store personal data in accordance with the agreement with the data controller.

No.	*SpeedAdmin ApS' control activity*	*Test performed by Grant Thornton*	*Result of test*
E.2	Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.	We have inspected that the data processor has a complete and updated list of processing activities stating localities, countries, or regions. We have, by sample test, inspected that documentation exists that the processing of data, including the storage of personal data, takes place only in the localities stated in the data processing agreement – or otherwise as approved by the data controller.	No deviations noted.

Control objective F – Use of sub-processors

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

No.	*SpeedAdmin ApS' control activity*	*Test performed by Grant Thornton*	*Result of test*
F.1	Written procedures exist which include requirements for the data processor when using sub-processors, including requirements for sub-data processing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place for using sub-processors, including requirements for sub-data processing agreements and instructions. We have inspected that procedures are up to date.	No deviations noted.
F.2	The data processor only uses sub-processors to process personal data that have been specifically or generally approved by the data controller.	We have inspected that the data processor has a complete and updated list of sub-processors used. We have, by sample test, inspected that documentation exists that the processing of data by the sub-processor is stated in the data processing agreements – or otherwise as approved by the data controller.	No deviations noted.

Control objective F – Use of sub-processors

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

No.	*SpeedAdmin ApS' control activity*	*Test performed by Grant Thornton*	*Result of test*
F.3	When changing the generally approved sub-processors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the data processor. When changing the specially approved sub-processors used, this has been approved by the data controller.	We have inquired about whether there have been changes to sub-data processors the past six months.	We have been informed that there have been no changes in the use of sub-processors within the last six months. No deviations noted.
F.4	The data processor has subjected the sub-processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	We have inspected the existence of signed sub-data processing agreements with sub-processors used, which are stated on the data processor's list. We have, by sample test, inspected that sub-data processing agreements include the same requirements and obligations as are stipulated in the data processing agreements between the data controllers and the data processor.	No deviations noted.
F.5	The data processor has a list of approved sub-processors.	We have inspected that the data processor has a complete and updated list of sub-processors used and approved. We have inspected that, as a minimum, the list includes the required details about each sub-processor.	No deviations noted.

Control objective F – Use of sub-processors

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

No.	*SpeedAdmin ApS' control activity*	*Test performed by Grant Thornton*	*Result of test*
F.6	Based on an updated risk assessment of each sub-processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity.	We have inspected that formalised procedures are in place for follow-up on processing activities by the sub-processors and compliance with the sub-data processing agreements. We have inspected documentation that the data processor has identified the processing that the individual subprocessor carries out on behalf of the data processor, including a description of the level of supervision of these. We have inspected documentation to show that proper follow-up has been carried out on technical and organisational measures, the processing security of the sub-processors used, the third country's basis for transfer, and the like.	No deviations noted.

Control objective G – Transfer of personal data to third countries

Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.

No.	*SpeedAdmin ApS' control activity*	*Grant Thornton's test*	*Result of test*
G.1	Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist to ensure that personal data are only transferred to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. We have inspected that procedures are up to date.	No deviations noted.
G.2	The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.	We have inspected that instructions on third-country transfers are stated in data processing agreements. We have inquired whether the data processor has transferred personal data to third countries or international organisations	We have been informed that personal data are not being transferred to third-country or international organisations. No deviations noted.
G.3	As part of the transfer of personal data to third countries or international organisations, the data processor assessed and documented the existence of a valid basis of transfer.	We have inquired whether the data processor has transferred personal data to third countries or international organizations.	We have been informed that personal data are not being transferred to third-country or international organisations. No deviations noted.

Control objective H – Rights of the data subjects

Procedures and controls are complied with to ensure that the data processor can assist the data controller in handing out, correcting, deleting, or restricting information on the processing of personal data to the data subject.

No.	*SpeedAdmin ApS' control activity*	*Test performed by Grant Thornton*	*Result of test*
H.1	Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects. We have inspected that procedures are up to date.	No deviations noted.
H.2	The data processor has established procedures as far as this was agreed that enable timely assistance to the data controller in handing out, correcting, deleting, or restricting or providing information about the processing of personal data to data subjects.	We have inspected that the procedures in place for assisting the data controller include detailed procedures for: • Handing out data • Correcting data • Deleting data • Restricting the processing of personal data • Providing information about the processing of personal data to data subjects. We have inspected documentation that the systems and databases used support the performance of the relevant detailed procedures.	No deviations noted.

Control objective I – Managing personal data breaches

Procedures and controls are complied with to ensure that any personal data breaches are responded to in accordance with the data processing agreement entered into.

No.	*SpeedAdmin ApS' control activity*	*Test performed by Grant Thornton*	*Result of test*
I.1	Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. We have inspected that procedures are up to date.	No deviations noted.
I.2	The data processor has established controls to identify any personal data breaches.	We have inspected that the data processor provides awareness training to employees in relation to the identification of any personal data breaches.	No deviations noted.
I.3	If any personal data breach occurred, the data processor informed the data controller without undue delay after having become aware of such personal data breach at the data processor or a sub-processor.	We have inspected that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach. We have inspected that the data processor has included any personal data breaches at sub-processors in the data processor's list of security incidents. We have inspected that all personal data breaches recorded at the data processor or the sub-processors, have been communicated to the data controllers concerned without undue delay after the data processor became aware of the personal data breach.	No deviations noted.

Control objective I – Managing personal data breaches

Procedures and controls are complied with to ensure that any personal data breaches are responded to in accordance with the data processing agreement entered into.

No.	*SpeedAdmin ApS' control activity*	*Test performed by Grant Thornton*	*Result of test*
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency: • Nature of the personal data breach • Probable consequences of the personal data breach • Measures taken or proposed to be taken to respond to the personal data breach.	We have inspected that the procedures in place for informing the data controllers in the event of any personal data breach include detailed procedures for: • Describing the nature of the personal data breach • Describing the probable consequences of the personal data breach • Describing measures taken or proposed to be taken to respond to the personal data breach. We have inspected documentation that the procedures available support that measures are taken to respond to the personal data breach.	No deviations noted.

PENNEO

The signatures in this document are legally binding. The document is signed using Penneo™ secure digital signature. The identity of the signers has been recorded, and are listed below.

"By my signature I confirm all dates and content in this document."

Michael Jørgen Hamann

Underskriver 1
Serial number: 097ddc41-cb32-4d8c-b13c-3465567f9658
IP: 46.32.xxx.xxx
2026-06-22 14:03:11 UTC

MitID

Martin Brogaard Borup Nielsen

Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Partner
Serial number: 658bcd61-1988-4367-b3eb-215cfbbb49b0
IP: 172.225.xxx.xxx
2026-06-22 14:33:11 UTC

MitID

Kristian Randløv Lydolph

Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Statsautoriseret revisor
Serial number: 84758c07-82ce-4650-a48d-5224b246b5c4
IP: 62.243.xxx.xxx
2026-06-22 15:17:52 UTC

MitID