



revi-it

Building a safer society through compliance

Assurance report

Let's Learn To Play! ApS SpeedAdmin

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with customers as of 21 June 2022

July 2022

REVI-IT A/S | www.revi-it.dk
Højbro Plads 10, 1200 København K
CVR: 30 98 85 31 | Tlf. 33 11 81 00 | info@revi-it.dk
www.dpo-danmark.dk | www.revi-cert.dk

Table of Contents

Section 1:	Let's Learn To Play! ApS' description of processing activity for the supply of the administration system SpeedAdmin to schools of music and culture	1
Section 2:	Let's Learn To Play! ApS' statement.....	6
Section 3:	Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to Let's Learn To Play! ApS' data processing agreement with customers	8
Section 4:	Control objectives, controls, tests, and results hereof.....	11

Amendment with Respect to Name Change

All references to "SpeedAdmin ApS" in this assurance report,
are hereby replaced with "Let's Learn to Play! ApS"

Section 1: Let's Learn To Play! ApS' description of processing activity for the supply of the administration system SpeedAdmin to schools of music and culture

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

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

The processing of personal data is performed according to the general agreement (license agreement) between Let's Learn To Play! ApS and the schools of music and culture, which is signed in the beginning of the consignment.

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

Description of processing

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

Personal data

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

Categories of data subjects included in the data processor agreement:

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

Practical measures

The management of Let's Learn To Play! ApS has approved all measures, internal standards, individual yearly audits, performed internally within Let's Learn To Play! ApS

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

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

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

Risk assessment

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

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

Changes in the risk assessment will always be approved and signed by one of Let's Learn To Play! ApS' managers.

Processing - instructions

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

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

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

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

Procedure review

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

Procedures – access management

Let's Learn To Play! ApS' management is in charge of decisions and the administration of which user accesses the individual employee should have.

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

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

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

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

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

Procedures – development

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

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

Procedures – managing personal data requests

Let's Learn To Play! ApS is not allowed to process personal data requests from data subjects. Since we are "only" the processor and therefore not data controller, we are not authorised to process these requests.

It is the role of the data controller – our customers, who are authorised to process personal data requests.

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

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

Procedures – security incidents

Let's Learn To Play! ApS is logging security incidents according to the internal standard about security incidents. Among other things, it is important that the DPO is included as soon as a security incident has been discovered.

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

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

Sub-processors

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

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

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

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

Unit IT:

SpeedAdmin uses Unit It to host servers. All data in SpeedAdmin's databases is stored on the servers of Unit IT. The data will be deleted as per the data processor agreement, when a customer terminates.

Unit IT is located at Strandvejen 7, 5500 Middelfart, Denmark. This means that Unit IT does not transfer data to other countries.

Link Mobility:

SpeedAdmin uses Link Mobility to send text messages through SpeedAdmin. The data that is sent from SpeedAdmin to Link Mobility is the messages incl. the mobile numbers. This data is stored on Link Mobility's server, which is located at Storsätragränd 3, 127 39 Skärholmen, Sweden. There is therefore no transfer to other countries.

Zendesk:

SpeedAdmin uses Zendesk as a support system. The data that will be in Zendesk is contact information (name and e-mail address) of the superuser who creates a ticket. It is the customers' superusers who are responsible for using the ID numbers SpeedAdmin uses on students, parents and teachers, if their inquiry concerns individuals. That way, no personal information will enter Zendesk.

Zendesk automatically deletes tickets older than 2 years.

SpeedAdmin's data in Zendesk is located in a data center in Ireland, but since Zendesk is an US-owned company, SpeedAdmin has chosen to take its precautions and assessed the risk of third country access to data. Zendesk has a valid transfer basis; Binding Corporate Rules (BCR). In addition, SpeedAdmin has prepared a TIA (Transfer Impact Assessment), where the assessment has showed that the risk of third countries having

access to data is very small and unlikely. SpeedAdmin also has internal standards that ensure that all employees act the same when it comes to subcontractors and a documented inspection of Zendesk is held annually.

Microsoft:

SpeedAdmin uses Microsoft for the mail system and the Teams function. Teams are used in the start-up and implementation of new customers and online meetings.

Data is stored within the EU. This is ensured every year when the subcontractor is supervised.

As with Zendesk, Microsoft is also a US-owned company. Therefore, the same measures and supervision have been taken as with Zendesk. Microsoft has approved EU standard contract terms (also known as EU model clauses), which is a valid transfer basis in case they should have access to data. But Microsoft will only access data if SpeedAdmin gives them access, which SpeedAdmin's internal standards have ensured does not happen.

The TIA prepared for Microsoft also shows a very small and unlikely risk that Microsoft would gain access to data.

Third countries

It has been decided that Let's Learn To Play! ApS neither store nor transfer data to third countries. Therefore, this is also an issue for inspection, before Let's Learn To Play! ApS decides to employ a new sub-processor.

Employees

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

Complementary controls

- Data controller is responsible for deleting the logs
- Superusers are the only ones authorized to anonymize users in the system
- In case the controller downloads Excel spreadsheets from SpeedAdmin, the controller is responsible for deleting it
- The controller must pay attention to the mails being sent by the system about locked users
- The Data Controllers have their own duty of information to the data subjects in SpeedAdmin – we naturally assist with information about the processing.
- The controllers themselves have duty of disclosure to the data subjects in SpeedAdmin – we of course assist with information about the processing.

Section 2: Let's Learn To Play! ApS' statement

Let's Learn To Play! ApS processes personal data in accordance with the data processing agreement with their customers.

The accompanying description has been prepared for data controllers, who has used administration system SpeedAdmin to schools of music and culture , and who has a sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the EU Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "the Regulation") have been complied with.

Let's Learn To Play! ApS uses the following sub-suppliers and sub-processors, Microsoft, Zendesk, Unit-IT and Link Mobility. Certain control objectives stated in the description can only be achieved, if the sup-supplier's controls as assumed in the design of our controls, are appropriately designed, and operationally implemented. This statement does not include control objectives and related controls at Let's Learn To Play! ApS' sub-suppliers and sub-processors.

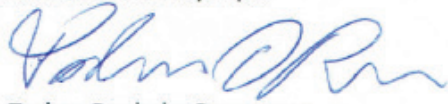
Some of the control objectives stated in Let's Learn To Play! ApS' description in Section 1, can only be achieved if the complementary controls with the customers have been appropriately designed and implemented with the controls with Let's Learn To Play! ApS. The report does not include the appropriateness of the design and implementation of these complementary controls

Let's Learn To Play! ApS confirms that:


- a) The accompanying description, Section 1, fairly presents administration system SpeedAdmin to schools of music and culture, which has processed personal data for data controllers subject to the Regulation as of 21 June 2022. The criteria used in making this statement were that the accompanying description:
 - (i) Presents how administration system SpeedAdmin to 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 administration system SpeedAdmin to schools of music and culture, 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 administration system SpeedAdmin to 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 administration system SpeedAdmin to 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 of 21 June 2022. 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, 4 July 2022
Let's Learn To Play! ApS



Torben Dueholm Rasmussen
CCO



Karsten Grau Rasmussen
CTO

Section 3: Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to Let's Learn To Play! ApS' data processing agreement with customers

To: Let's Learn To Play! ApS and their customers

Scope

We were engaged to provide assurance about a) Let's Learn To Play! ApS' description, Section 1, of administration system SpeedAdmin to schools of music and culture, in accordance with the data processing agreement with customers as data controllers as of 21 June 2022 and about b) the design and implementation of controls related to the control objectives stated in the Description.

Let's Learn To Play! ApS uses the following sub-suppliers and sub-processors, Microsoft, Zendesk, Unit-IT and Link Mobility. Certain control objectives stated in the description can only be achieved, if the sub-supplier's controls as assumed in the design of our controls, are appropriately designed, and operationally implemented. This statement does not include control objectives and related controls at Let's Learn To Play! ApS' sub-suppliers and sub-processors.

Some of the control objectives stated in Let's Learn To Play! ApS' description in Section 1, can only be achieved if the complementary controls with the customers have been appropriately designed and implemented with the controls with Let's Learn To Play! ApS. The report does not include the appropriateness of the design and implementation of these complementary controls

We express reasonable assurance in our conclusion.

Let's Learn To Play! ApS' responsibilities

Let's Learn To Play! ApS is responsible for: preparing the Description and the accompanying statement, Section 2, 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.

Our 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 behavior and ethical requirements applicable to Denmark.

REVI-IT A/S is subject to the International Standard on Quality Control (ISQC 1) and accordingly uses and 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.

Auditor's responsibilities

Our responsibility is to express an opinion on Let's Learn To Play! 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 administration system SpeedAdmin to 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

Let's Learn To Play! ApS' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of administration system SpeedAdmin to 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. In our opinion, in all material respects:

- (a) The Description fairly presents administration system SpeedAdmin to schools of music and culture as designed and implemented as of 21 June 2022; and
- (b) The controls related to the control objectives stated in the Description were appropriately designed as of 21 June 2022.

Description of tests of controls

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

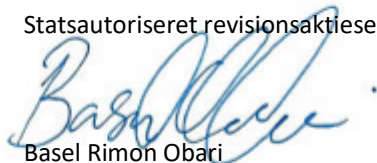
Intended users and purpose

This report and the description of tests of controls in Section 4 are intended only for data controllers who have used Let's Learn To Play! ApS' administration system SpeedAdmin to 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.

Copenhagen, 4 July 2022

REVI-IT A/S

Statsautoriseret revisionsaktieselskab



Basel Rimón Obari
Partner, CISA, CISM



Michael Marseen
Statsautoriseret revisor

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

We have 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 below. Our test has included the controls, we find necessary to establish reasonable assurance for compliance with the articles stated as of 21 June 2022.

Our statement, does not apply to controls, performed at Let's Learn To Play! ApS' sub-suppliers and sub-processors.

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

We performed our test of controls at Let's Learn To Play! ApS by the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at Let's Learn To Play! ApS. The interviews have included questions about, how controls are performed.
Observation	Observing how controls are performed.
Inspection	Reading of documents and reports, including description of the performance of the control. This includes reading and assessment of reports and documents to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented.
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
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	<i>New scope compared to ISO 27001/2</i>
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	<i>New scope compared to ISO 27001/2</i>
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	<i>New scope compared to ISO 27001/2</i>
D.1	6, 11, 13 , 14 , 32	7.4.5 , 7.4.7 , 7.4.4	<i>New scope compared to ISO 27001/2</i>
D.2	6, 11, 13, 14, 32	7.4.5 , 7.4.7 , 7.4.4	<i>New scope compared to ISO 27001/2</i>
D.3	13, 14	7.4.7 , 7.4.4	<i>New scope compared to ISO 27001/2</i>
E.1	13, 14, 28 , 30	8.4.2 , 7.4.7 , 7.4.8	<i>New scope compared to ISO 27001/2</i>
E.2	13, 14, 28 , 30	8.4.2 , 7.4.7 , 7.4.8	<i>New scope compared to ISO 27001/2</i>
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

Control activity	GDPR articles	ISO 27701	ISO 27001/2
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	<i>New scope compared to ISO 27001/2</i>
H.2	12, 13, 14 , 15, 20, 21	7.3.5, 7.3.8, 7.3.9	<i>New scope compared to ISO 27001/2</i>
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.	Let's Learn To Play! ApS' control activity	Test performed by REVI-IT A/S	Result of test
A.1	<p>Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have inspected that formalised procedures exist to ensure that personal data are only processed according to instructions.</p> <p>We have inspected that procedures are up to date.</p>	No deviations noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	We have by sample test inspected data processor agreements and by sample test ensured that the processor only processes personal data in accordance with the 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 formalized procedures exist ensuring verification that personal data are not processed in violation of the Regulation or other legislation.	<p>We have been informed that there have been no instructions that has been deemed unlawful by the data processor and we have therefore not been able to test the implementation of the data processors controls.</p> <p>No deviations noted.</p>

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.	Let's Learn To Play! ApS' control activity	Test performed by REVI-IT A/S	Result of test
B.1	<p>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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have inspected that formalised procedures exist to ensure establishment of the safeguards agreed.</p> <p>We have inspected that procedures are up to date.</p>	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 by sample test inspected a server and by sample test ensured that antivirus is implemented and updated.	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 by sample test inspected the implementation of firewall, including the configuration.	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 inspected network diagrams and other network documentation to ensure appropriate segmentation.	No deviations noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	<p>We have inspected, that formalized procedures for limiting user access to personal data, have been established.</p> <p>We have by sample test inspected the access rights of a new employee to ensure, that these are based on a work-related need.</p>	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.	Let's Learn To Play! ApS' control activity	Test performed by REVI-IT A/S	Result of test
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 by sample test inspected surveillance and alarms on systems.	No deviations noted.
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	We have by sample test inspected transmission of personal data over the internet and by sample test ensured that the transmissions are encrypted.	No deviations noted.
B.9	Logging has been established in systems, databases, and networks. Logon data are protected against manipulation and technical errors and are reviewed regularly.	We have inspected the policy for logging and ensured that decisions have been made to protect personal data. We have, by sample test, inspected the set-up of system loggings and we have ensured that this complies with the policy.	No deviations noted.
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, by sample test, inspected the development server and ensured that the data set is anonymized.	No deviations noted.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	We have by inspected penetration test and inquired about how it is ensured that vulnerabilities are being handled.	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 the procedure for changes. We have by sample test inspected changes and by sample test ensured that changes follow the procedure.	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.	Let's Learn To Play! ApS' control activity	Test performed by REVI-IT A/S	Result of test
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.	<p>We have inspected that formalised procedures exist for granting and removing users' access to systems and databases using to process personal data.</p> <p>We have by sample test inspected accesses rights and by sample test ensured that the users have a work-related need.</p> <p>We have by sample test inspected accesses and by sample test ensured that new employees have been allocated according to the procedure.</p> <p>We have inquired about resignations.</p> <p>We have inspected that documentation is available of regular – and minimum once a year – review and approval of allocated user accesses.</p>	No deviations noted.
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 by sample test inspected that users' access to personal data take place 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 access to the data processor's office is being reviewed.	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.	Let's Learn To Play! ApS' control activity	Test performed by REVI-IT A/S	Result of test
C.1	<p>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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.</p>	<p>We have inspected that an information security policy exists that Management has considered and approved within the past year.</p> <p>We have ensured, that the information security policy is available to the employees.</p> <p>We have inspected the control of information security policy and ensured that this is regularly assessed.</p>	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 inspected documentation that the data processor regularly evaluates the information security policy and we have ensured that it follows the data processor agreements.	No deviations noted.
C.3	The employees of the data processor are screened as part of the employment process.	<p>We have inspected that formalised procedures are in place to ensure screening of the data processor's employees as part of the employment process.</p> <p>We have by sample test inspected documentation for the screening of an employee</p>	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.	<p>We have, by sample test, inspected that a new employee has signed a non-disclosure agreement.</p> <p>We have by sample test inspected that a new employee has been introduced to relevant procedures and policies.</p>	No deviations noted.
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.	<p>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 being returned.</p> <p>We have inquired about resignations.</p>	<p>We have been informed that there have been no resignations, which is why we have not tested the implementation of relevant procedures.</p> <p>No deviations noted.</p>

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.	Let's Learn To Play! ApS' control activity	Test performed by REVI-IT A/S	Result of test
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 inquired about resignations.	We have been informed that there have been no resignations, wherefore we have not tested the implementation of relevant procedures. 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.	No deviations noted.
C.8	The processor has assessed the need for a DPO and has ensured that the DPO has the adequate professional competence to perform their tasks and are involved in relevant areas.	We have, by sample test, inspected controls and procedures and ensured that the DPO has been involved.	No deviations noted.
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. Management has ensured that the record of categories of processing activities for each controller is adequate, updated, and correct.	We have inspected that there are records that the management has processed and approved within the past year.	No deviations noted.

Control objective D - Return and deletion of personal data

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

No.	Let's Learn To Play! ApS' control activity	Test performed by REVI-IT A/S	Result of test
D.1	<p>Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have inspected that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller.</p> <p>We have inspected that the procedures are up to date.</p>	No deviations noted.
D.2	Specific requirements have been agreed with respect to the data processor's storage periods and deletion routines.	We have, by sample test, inspected a new data processing agreement, and ensured that decisions have been made about storage periods and deletion routines.	No deviations noted.
D.3	<p>Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been:</p> <ul style="list-style-type: none"> Returned to the data controller; and/or Deleted if this is not in conflict with other legislation. 	<p>We have inspected that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data.</p> <p>We have, by sample test, inspected that documentation exists that the agreed deletion or return of data has taken place for terminated data processing sessions.</p>	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.	Let's Learn To Play! ApS' control activity	Test performed by REVI-IT A/S	Result of test
E.1	<p>Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have inspected that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements.</p> <p>We have inspected that the procedures are up to date.</p>	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.	Let's Learn To Play! ApS' control activity	Test performed by REVI-IT A/S	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 by sample test inspected data processing agreements and by sample test ensured that personal data is only stored at approved locations. We have by sample test inspected the backup implementation.	No deviations noted.

Control objective F – Use of sub-processors

Procedures and controls are complied with to ensure that only approved sub-data 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.	Let's Learn To Play! ApS' control activity	Test performed by REVI-IT A/S	Result of test
F.1	Written procedures exist which include requirements for the data processor when using sub-data 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 processing agreements and instructions. We have inspected that procedures are up to date.	No deviations noted.
F.2	The data processor only uses sub-data processors to process personal data that have been specifically or generally approved by the data controller.	We have by sample test inspected processing agreement and ensured that the processor either has a general or a specific authorization to use sub processors.	No deviations noted.
F.3	When changing the generally approved sub-data 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-data processors used, this has been approved by the data controller.	We have inquired about new sub processors.	We have been informed that there have not been any new sub processors, so we have not been able to test the implementation of the data processors processes. No deviations noted.

Control objective F – Use of sub-processors

Procedures and controls are complied with to ensure that only approved sub-data 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.	Let's Learn To Play! ApS' control activity	Test performed by REVI-IT A/S	Result of test
F.4	The data processor has subjected the sub-data processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	We have by sample test inspected data processing agreements with new sub-processors and by sample test ensured that the sub-processor is committed to same or similar data protection obligations as the controller.	No deviations noted.
F.5	The data processor has a list of approved sub-data processors.	We have inspected the list of sub-processors and ensured that all relevant sub-processors are stated in the list.	No deviations noted.
F.6	Based on an updated risk assessment of each sub-data 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. The data controller is informed of the follow-up performed at the sub-data processor.	<p>We have by sample test inspected that the processor has reviewed sub processors and collected relevant material.</p> <p>We have inspected documentation that each sub-data processor and the current processing activity at such processor are subjected to risk assessment.</p> <p>We have inspected documentation that technical and organisational measures, security of processing at the sub-data processors used, third countries' bases of transfer and similar matters, are appropriately followed up on.</p> <p>We have inspected of documentation that information on the follow-up at sub-data processors is communicated to the data controller enabling the controller to plan an inspection.</p>	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.	Let's Learn To Play! ApS' control activity	Test performed by REVI-IT A/S	Result of test
G.1	<p>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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have by sample test inspected data processing agreement and ensured that transfer of personal data to third countries has been addressed.</p> <p>We have inquired about transfer of personal data to third countries.</p>	<p>We have been informed that the data processor does not transfer personal data to third countries, and we find this plausible based on our tests.</p> <p>No deviations noted.</p>
G.2	<p>The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.</p>	<p>We have by sample test inspected data processing agreement and ensured that transfer of personal data to third countries has been addressed.</p> <p>We have inquired about transfer of personal data to third countries.</p>	<p>We have been informed that the data processor does not transfer personal data to third countries, and we find this plausible based on our tests.</p> <p>No deviations noted.</p>
G.3	<p>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.</p>	<p>We have by sample test inspected random data processor agreement and ensured transfer to third countries has been addressed.</p> <p>We have inquired about transfer of personal data to third countries.</p>	<p>We have been informed that the data processor does not transfer personal data to third countries, and we find this plausible based on our tests.</p> <p>No deviations noted.</p>

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.	Let's Learn To Play! ApS' control activity	Test performed by REVI-IT A/S	Result of test
H.1	<p>Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>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.</p> <p>We have inspected that procedures are up to date.</p>	No deviations noted.
H.2	The data processor has established procedures in so 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.	<p>We have inquired if there have been any requests.</p> <p>We have by sample test inspected technical documentation for that requests can be managed.</p>	<p>We have been informed that no assistance has been handled in relation to requests within the last year.</p> <p>No deviations noted.</p>

Control objective I – Managing personal data breaches

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

No.	Let's Learn To Play! ApS' control activity	Test performed by REVI-IT A/S	Result of test
I.1	<p>Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>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.</p> <p>We have inspected that procedures are up to date.</p>	No deviations noted.
I.2	<p>The data processor has established the following controls to identify any personal data breaches:</p> <ul style="list-style-type: none"> • Awareness of employees • Monitoring of network traffic • Follow-up on logging of access to personal data. 	We have inspected that the data processor provides awareness training to the employees in identifying 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-data processor.	<p>We have inspected that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach.</p> <p>We have inquired about data breaches.</p>	<p>We have been informed that there has been no data breach and we have therefore not been able to test the implementation of the data processor's procedures.</p> <p>No deviations noted.</p>
I.4	<p>The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency:</p> <ul style="list-style-type: none"> • 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 the procedure and ensured that assistance to the controller has been established.	No deviations noted.