revi-it

A safe society with IT and data

Assurance report

CVR No.: 25 89 69 39

TimeLog A/S

Independent auditor's ISAE 3000 assurance report with high degree of security related to compliance with the general data protection regulation (GDPR) and appurtenant data protection legislation in the role of data processor for the delivery of TimeLog PSA as of 25 April 2021.

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

April 2021

Table of contents

Section 1: TimeLog A/S' description

TimeLog A/S' description and internal controls

Introduction

This description concerns controls related to data protection and personal data with TimeLog. The purpose of this description is to provide information to TimeLog A/S' customers and their stakeholders about the requirements and contents of EU's General Data Protection Regulation "GDPR".

Further, the purpose of this description, is to provide information of questions regarding processing security, technical and organisational measures, responsibilities between data controller, our customers and data processor TimeLog, and how the services offered can support the data subjects' rights.

TimeLog uses GlobalConnect A/S as sub-supplier of data centre and infrastructure, from which TimeLog A/S' customers are operated. GlobalConnect is responsible for the physical security, hardware, network, backup and storage. GlobalConnect's latest ISAE 3402-II assurance report is from 2020.

Our control objectives, including rules, procedures and controls

TimeLog PSA is a focused, ambitious consultancy firm with a desire to develop business and optimize internal work procedures from contract to invoice. TimeLog develops and sells own software, used by our customers for optimizing their business through structured time recording, financial project management, competent resource management, invoicing and integration with the customer's other systems.

The data controller has acquired license for TimeLog's PSA-platform, where the data controller using the software, imports and then enters data, including personal data, to the software to plan time and resources within the data controller's organisation.

Principles regarding processing of personal data

In connection with the delivery of TimeLog's software solution, TimeLog processes personal data on behalf of the data controller according to current rules and in compliance with signed data processing agreement.

Our customer's trust and confidence in our ability to provide our services in a secure and confidential way is crucial to our business. Therefore, we take data protection and GDPR very seriously, and we continuously process customer data based on both technical and organisational measures.

Risk management in TimeLog

TimeLog has prepared a risk assessment to document the company's risk-based approach to the choice of security measures for the protection of physical persons in connection with the processing of personal data and the free movement of such data.

The purpose of the risk assessment is therefore to ensure that TimeLog's procedures and implemented security measures complies with the risks that TimeLog's processing of personal data causes the data subjects. By assessment of TimeLog's relevant risk and threat-categories, existing and already implemented security measures have been considered and we therefore refer to further statement on this.

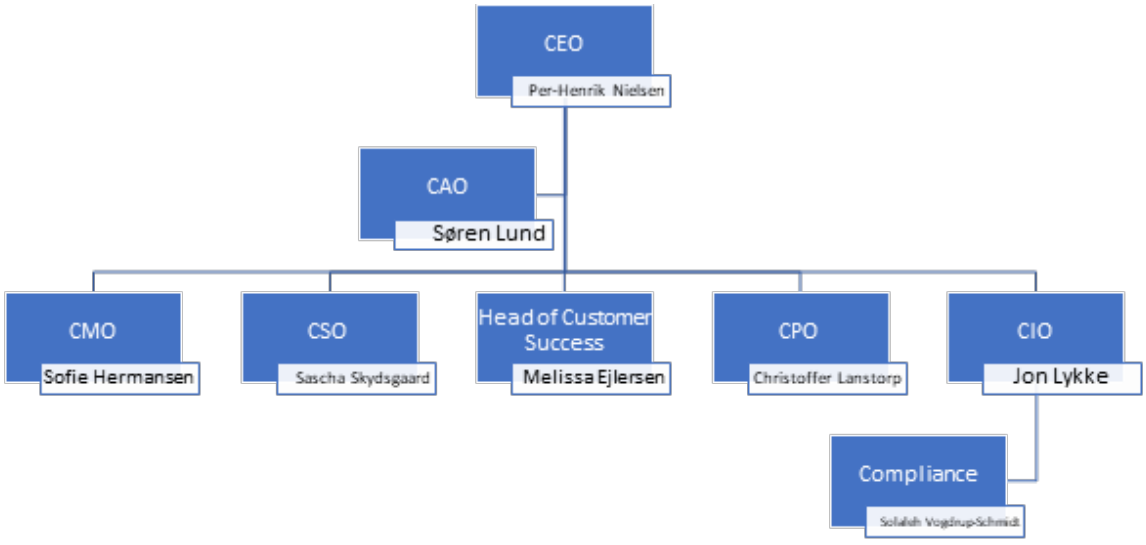
The risk assessment is based on the recommendations of the Danish Data Protection Agency, the Danish Business Authority and the Danish Council for Digital Security. The methodology follows the process, which is a part of, and the basis for the data controllers work with security standard ISO/IEC 27002, just like the risk assessment includes risk and threats, underlying the control objectives of the standard requirements ISO/IEC 27701 and the auditing standard ISAE 3000.

The risk assessment has been prepared, based on the following:

- Relevant risks and threats: the risk assessment covers the relevant risks and threats, point for point.
- Impact assessment: for every risk and threat category, the expected consequences of loss of confidence, accessibility or integrity have been assessed. The impact assessment can be high, medium or low.
- Probability: for every risk and threat category, the expected probability for loss of confidence, accessibility or integrity have been assessed concerning the relevant risk and threat category. The probability assessment does not cover already implemented security measures, since these subsequently are described and included in the risk picture. The vulnerability assessment or the probability assessment can be high, medium or low.
- Implemented security measures: TimeLog's implemented security measures are listed and described under each subject for the risk- and threat categories.
- Remaining risk: Finally, the remaining risk is assessed, based on the risk picture and the implemented security measures. This way, it is assessed, whether the implemented security measures are adequate, or whether further measures should be implemented. The remaining risk can be said to be calculated based on the following "formula" (consequence X probability) – existing measures = remaining risk. Risk assessment is updated at least annually, and whenever it is considered relevant.

Organisation and responsibility

TimeLogs organisation and management is based on a structure, classified by function, where the individual department managers are responsible for the staff. Further the manager is responsible for the documentation of the individual processes with the employees.



GDPR and TimeLogs role and responsibility as processor

The role of the data controller and the data processor and their responsibilities regarding processing of personal data follows the data processing agreement, entered by the parties.

In connection with the delivery of TimeLog's software solution, TimeLog is processing personal data on behalf of the data controller, according to applicable rules and signed data processing agreement.

The processing of personal data can only take place according to documented instructions from the data controller and can only concern the assignments, that TimeLog has according to the data processing agreement and the general agreement.

TimeLog has procedures and controls to ensure that TimeLog in due time can assist the data controller in handing over, correct, delete or limit the information about the data processing to the data subjects, to the extent agreed with the data controller, including procedures for:

- Handover of data
- Correction of data
- Data erasure
- Limitation in personal data processing
- Information about personal data processing to the data subject

Access to personal data is limited to users with a work-related need and TimeLog's IT-systems administration review this on an ongoing basis to ensure, that the agreed technical measures support the maintenance of the limitation in users' work-related access to personal data.

Personal data used for development, test or the like, are always in pseudonymized or anonymized form, when these are accessed by TimeLog's offshore development team. The use can only be to protect the data controller's purpose according to the existing data processing agreement, on behalf of same and in accordance with existing legislation.

Consent

TimeLog's processing is not based on consent, and since basis for processing is covered by an agreement, TimeLog is not responsible for obtaining consent. However, in support cases, TimeLog will always obtain customer's consent to access customer's data.

Processing of different categories of personal data

TimeLog may obtain and process personal data with the following purpose:

1. To perform the services, described in the contract for the use of TimeLog's software
2. Other purposes, according to written instructions from data controller

TimeLog processes personal data in compliance with the company's data processing agreement. Personal data, can be divided into two categories:

<u>General personal data, which i.a. can include:</u>

- Name
- Title
- E-mail
- Address
- Telephone
- Social media
- Date of birth
- Expenses
- Travel information
- Registration of work hours and normal absence

Sensitive personal data

- Health details
- Registration of absence due to illness
- Criminal offences

TimeLog has no way of controlling, what is written in free text fields and attached documents.

Data subjects' rights

TimeLog has a procedure for managing and documenting the inquiries from the data controller, related to assisting data controller with the handling of data subjects' rights.

A few of the data subjects' rights must be addressed on TimeLog's own initiative, whereas other rights are only addressed, upon request from data subjects. Therefore, TimeLog has very clear procedures describing how requests from data subjects are handled, including the deadlines for reply, making us able to observe the data subjects' rights.

Documentation of inquiries from data controller about e.g., access, deletion, correction, limitation of processing, data portability etcetera, is handled in our support system. TimeLog will – depending on the type of processing – assist the data controller using suitable technical and organisational measures to fulfil the data controller's obligation to reply to requests about the exercising of the data subjects' rights according to the Data Protection Act. TimeLog must supply any information requested by the data controller, within a reasonable timeframe.

Immediately after being made aware, TimeLog must – in writing – inform the data controller about any suspicion about or ascertainment of (i) data security breaches or (ii) accidental or unlawful destruction, loss, change, unauthorized disclosure of, or access to personal data processed by TimeLog. Further, TimeLog is under an obligation to inform the Danish Data Protection Agency, provided that the extent is assessed to be significant.

TimeLog must cooperate and assist the data controller in connection with the remedy of data security breaches.

General obligations as processor

The processing of personal data can only be performed according to documented instructions from the data controller and must only concern the assignments, TimeLog has undertaken according to the data processing agreement and the general agreement. Such instructions are normally available as appendixes to the existing data processing agreement with the data controller.

Data protection officer (DPO)

At present, TimeLog does not employ a Data Protection Officer (DPO) since the company's core business does not include personal data processing. However, TimeLog has a function; Data Security and Compliance Specialist, who manages DPO related tasks. On an annual basis, TimeLog will assess whether it is necessary to employ an internal or external DPO.

Transfer of personal data

Data processor can only process personal data according to the documented, written instructions from the data controller, unless processing is required according to EU-law or member states' national law to which the data processor is submitted.

Data processor cannot – in any way – change the contents of personal data or pass on personal data to third party, unless it is specifically mentioned in the data processing agreement between the data controller and the data processor, the data controller in other ways, in writing has authorised the data processor and/or instructions hereof and/or the handing over of data is required according to existing legislation, to which the data processor is submitted. I such cases, the data processor must inform the data controller, before commencing processing of personal data.

Full transparency for data controllers and data subjects

TimeLog has a written procedure, in which the following principles for processing of personal data according to data subjects' rights, have been decided upon:

- Legality, fairness and transparency
- Limited purpose
- Data minimisation
- Accuracy
- Limited storing
- Integrity and confidentiality

An ongoing assessment is made, as of whether the described procedures need to be updated to be in accordance with the above principles.

Complementary controls with the data controller

As part of the services, there are controls expected to be implemented by the data controller and which are of significance to obtain the control objectives, described in the description. The data controller is under obligation to ensure the following:

- That the use of TimeLog's solution is only according to the types of data subjects and categories of personal data included in the data processing agreement signed by the parties
- That the data controller's personal data, and users are updated, including which personal data the system must include
- That given instructions are legal, related to the personal data legislation, in force at any time
- That the instruction to the data controller is appropriate, compared to the data processing agreement and the principal service
- That decisions have been made to the consequences related to protection of information privacy upon request for changes
- That sensitive personal data are not transmitted to TimeLog in support cases, via tickets etcetera

Section 2: TimeLog A/S' statement

The accompanying description has been prepared for TimeLog A/S' customers, who, in the role as data controller has used TimeLog PSA, 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 omen the free movement of such data (hereinafter "the Regulation") have been complied with.

TimeLog A/S uses the following sub-suppliers, GlobalConnect A/S, Zendesk Inc, WalkMe Ltd, InScale, Hubspot Ireland Limited, Microsoft Ireland og Amazon Webservice. This assurance report has been prepared according to the carve-out method and does not include control objectives with sub-suppliers.

TimeLog A/S confirms that:

a) The accompanying description, Section 1, fairly presents TimeLog PSA, which has processed personal data for data controllers subject to the Regulation throughout the period from as of the 25 April 2021. The criteria used in making this statement were that the accompanying description:

   (i) Presents how TimeLog PSA 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 TimeLog PSA's, 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) Includes relevant information about changes in data controller's TimeLog PSA in the processing of personal data as of 25 April 2021.

(iii) Does not omit or distort information relevant to the scope of TimeLog PSA 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 TimeLog PSA 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 operated effectively as of 25 April 2021. 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

(ii) The identified controls would, if operated 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

Copenhagen, 30 April 2021

TimeLog A/S

Per Henrik Nielsen

Per-Henrik Ole Nielsen
CEO

Section 3: Independent auditor's ISAE 3000 assurance report with assurance on information security and measures pursuant to data processing agreement with customers as of 25 April 2021

To TimeLog A/S' management and the company's customers in the role of data controller.

Scope

We here engaged to provide assurance with high degree of assurance about TimeLog A/S' description in "Section" of TimeLog PSA, according to data processing agreements with their customers, in the role of data controller as of 25 April 2021 and of the design and implementation of controls, related to the control objectives stated in the description.

TimeLog A/S uses the sub-suppliers, GlobalConnect A/S, Zendesk Inc, WalkMe Ltd, InScale, Hubspot Ireland Limited, Microsoft Ireland og Amazon Webservice. This assurance report has been prepared according to the carve-out method and does not include control objectives at the sub-suppliers.

TimeLog A/S' responsibilities

TimeLog 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, implementing and effectively operating controls to achieve the stated control objectives.

Auditor's independence and quality control

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by FSR - Danish Auditors (Code of Ethics for Professional Accountants), which are based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional conduct.

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.

Our responsibilities

Our responsibility is to express an opinion on TimeLog A/S' Description and on the design and operating effectiveness 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 operating effectively.

An assurance engagement to report on the Description, design, and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of its [e.g., anonymization tool, digital timetable, or a specific hosting system] and about the design and operating effectiveness 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 or operating effectively. Our procedures included testing the operating effectiveness 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

TimeLog A/S' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of TimeLog PSA, 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, based on the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the management statement (section 2)

It is our opinion, in all material respects:

(a) The Description fairly presents TimeLog PSA as designed and implemented as of 25 April 2021, and

(b) That the controls related to the control objectives stated in the Description were appropriately designed as of 25 April 2021

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 TimeLog A/S' TimeLog PSA, 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, 30 April 2021

REVI-IT A/S
State-authorised public accounting company

Henrik Paaske
State-authorised public accountant

Christian H. Riis
CISA, Partner

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

The following summary has been prepared to create an overview of the controls, implemented by TimeLog A/S to comply with the General Data Protection Regulation (GDPR) and related data protection law.

TimeLog A/S uses the sub-suppliers, GlobalConnect A/S, Zendesk Inc, WalkMe Ltd, InScale, Hubspot Ireland Limited, Microsoft Ireland og Amazon Webservice. This assurance report has been prepared according to the carve-out method and does not include control objectives at the sub-suppliers.

The requirements, stated in law or legislation cannot be deviated from. On the other hand, it can be adjusted how security is implemented, since the security requirements in the legislation is of more general and overall nature, which among other things must consider purpose, nature of processing, the type of personal data etcetera. Further specific requirements in the individual customer agreements, can extend beyond the general requirements of the data protection regulation. In which cases these are not included in the following.

Controls, performed at TimeLog A/S's customers are not included in this statement, as the customers' own auditors must perform this review and assessment.

We have performed our test of controls at TimeLog A/S by the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at TimeLog A/S. 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 the 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 objective	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**	*New area according 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 area according 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
D.1	6, 11, **13, 14,** 32	**7.4.5**, **7.4.7**, 7.4.4	*New area according to ISO 27001/2*
D.2	6, 11, 13, 14, **32**	**7.4.5**, **7.4.7**, 7.4.4	*New area according to ISO 27001/2*
D.3	13, **14**	**7.4.7**, 7.4.4	*New area according to ISO 27001/2*
E.1	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*New area according to ISO 27001/2*
E.2	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*New area according 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

Control objective	GDPR-articles	ISO 27701	ISO 27001/2
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 area according to ISO 27001/2*
H.2	12, **13, 14,** 15**,** 20**,** 21	**7.3.5, 7.3.8, 7.3.9**	*New area according 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
J.1	**7,** 9, **13, 14**, 18	**7.2.4**, 7.3.4	*New area according to ISO 27001/2*
J.2	7, 14, 18	**7.3.4**	*New area according to ISO 27001/2*
J.3	11, 13, 14, 15, 17, 18, 21 28	**7.3.2, 8.2.5, 8.3.1, 8.5.4, 8.5.6**	*New area according to ISO 27001/2*
J.4	11, 13, 14, 15, 17, 18, 21 28	**7.3.2, 8.2.5, 8.3.1, 8.5.4, 8.5.6**	*New area according to ISO 27001/2*
K.1	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 area according to ISO 27001/2*
K.2	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 area according to ISO 27001/2*
K.3	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 area according to ISO 27001/2*

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 consistent with the signed data processing agreement.

No.	Data processor's control activity	Test performed by REVI-IT A/S	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 the information security policy and ensured that it has been decided that processing must follow instructions from data controller. We have inspected the ongoing control of the policy and ensured that it is updated at least once a year.	No deviations noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller	We have inspected the information security polity and – by sample test – ensured that this follows data processing agreements.	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 the process for handling instructions and ensured that illegal instructions are being addressed.	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.	Data processor's control activity	Test performed by REVI-IT A/S	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.	We have inspected the information security policy and ensured that it has been decided to follow data processing agreements.	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 the antivirus software, and – by sample test – ensured that this is implemented and updated.	No deviations noted.

No.	Data processor's control activity	Test performed by REVI-IT A/S	Result of test
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 firewall setup and – by sample test – ensured that this has been configured in accordance with 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 – by sample test – inspected network components and – by sample test – insured that the network is properly segmented.	No deviations noted.
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 – by sample test – inspected accesses and – by sample test – ensured that access is based on a work-related need.	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.	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 encryption of laptops and – by sample test – ensured that these has been properly configured. We have – by sample test – inspected the transfer of personal data and – by sample test – ensured that this is protected by a powerful encryption.	No deviations noted.
B.9	Logging has been established in systems, databases and networks.	We have – by sample test – inspected the log setup of network components and – by sample teat – ensured that this has been configured according to internal policies.	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 personal data, and – by sample test – ensured that production data are not used for testing.	No deviations noted.

No.	Data processor's control activity	Test performed by REVI-IT A/S	Result of test
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	We have inspected the information security policy and ensured, that ongoing test of systems has been decided upon. We have – by sample test – inspected ongoing system testing and – by sample test – ensured that this has been performed during the period.	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 change procedure and ensured that changes are following formalized procedures. We have – by sample test – inspected changes and – by sample test ensured that these follow the procedure.	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 – by sample test – inspected accesses. 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.
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 accesses to personal data and – by sample test – ensured that this only takes place by using two-factor authentication.	No deviations noted.
B.15	Physical access safeguards have been established to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed.	We have inspected lists of key fobs 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.	Data processor's control activity	Test performed by REVI-IT A/S	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 written information security policy exists, that management has discussed and approved within the last year. We have inspected the control and ensured that the policy is updated on an ongoing basis. We have inspected documentation that information security policy has been communicated to relevant stakeholders, including 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.	We have – by sample test – inspected the information security policy and data processing agreements and – by sample test – ensured that they agree.	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.	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 – by sample test – inspected employment contracts and – by sample test – ensured that non-disclosure agreements have been signed. We have inspected the recruitment procedure and ensured that new employees have been introduced to policies and procedures.	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.	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 - by sample test - inspected that rights have been deactivated or terminated.	No deviations noted.

No.	Data processor's 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 – by sample test – inspected employment contracts, and – by sample test – ensured that confidentiality remains valid after termination.	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 documentation that data processor has planned awareness training of employees.	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 documentation of the data controller having assessed the need for a data protection officer.	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.	Data processor's control activity	Test performed by REVI-IT A/S	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 – by sample test – inspected data processing agreements, and – by sample test – ensured that storage periods and deletion routines have been decided upon.	No deviations noted.
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 – by sample test – inspected technical documentation supporting the procedures.	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.	Data processor's control activity	Test performed by REVI-IT A/S	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 the procedures and ensured, that the data processor ensures that personal data are stored according to the contract. We have inspected the procedures and ensured that they are updated.	No deviations noted.
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 processing only takes place on agreed locations.	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.	Data processor's 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-data 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-data 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-data processors used. We have – by sample test – inspected data processing agreements and – by sample test – ensured that the data processor has a general or specific authorisation to use sub-suppliers.	No deviations noted.

No.	Data processor's control activity	Test performed by REVI-IT A/S	Result of test
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 – by sample test – inspected data processing agreements and ensured that the data processor has been told to inform data controller when changing the sub-data processors used.	No deviations noted.
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 and sub-data processing agreements, and – by sample test – ensured that they include the same or similar requirements as imposed on the data processor.	No deviations noted.
F.5	The data processor has a list of approved sub-data processors.	We have – by sample test - inspected data processing agreements and – by sample test – ensured that they include relevant sub-data processors.	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.	We have inspected the ongoing control of sub-data processors and ensured that this is performed regularly.	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.	Data processor's control activity	Test performed by REVI-IT A/S	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 – by sample test – inspected data processing agreements and – by sample test – ensured that the data processor only transfer data to third countries according to instructions.	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 inspected documentation that transfer to third countries is performed on a valid basis of transfer.	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.	Data processor's control activity	Test performed by REVI-IT A/S	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 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.	We have inspected the procedures for assisting the data controller in due time. We have – by sample test – inspected documentation that the underlying systems support the procedures.	No deviations noted.

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.	Data processor's control activity	Test performed by REVI-IT A/S	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 controller has planned awareness controls to prevent possible 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.	We have inspected the procedure and incident logs and ensured that the data controller will be informed of potential data breaches.	No deviations noted.

No.	Data processor's control activity	Test performed by REVI-IT A/S	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 the procedure and ensured that the procedure includes requirements of assistance to the data controller when reporting to the Data Protection Agency.	No deviations noted.

Control objective J – Conditions for consent and duty of disclosure

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

No.	Data processor's control activity	Test performed by REVI-IT A/S	Result of test
J.1	There are written procedures for the obtaining of written consent for the processing of personal data Regularly – an at least annually – a assessment is made of whether the procedures need to be updated.	We have inquired into whether TimeLog is obtaining consent on behalf of the data controller.	We have been informed, that TimeLog does not obtain consent on behalf of the data controller. No deviations noted.
J.2	Technical measures have been implemented that ensure that it can be documented what information has been provided in connection with the giving of consent.	We have inquired into whether TimeLog is obtaining consent for processing on behalf of the data controller.	We have been informed, that TimeLog does not obtain consent on behalf of the data controller. No deviations noted.
J.3	There are written procedures in which it is described how it is ensured that the data subject receives information on the purpose of the processing of personal data as well as information on any transfer of personal data to recipients, third countries, or international organisations, or how the processor can assist the controller with this. Regularly – and at least annually – assessment is made of whether the procedures need to be updated.	We have inquired into whether TimeLog is responsible for the duty of disclosure.	We have been informed, that TimeLog is not responsible for the duty of disclosure. No deviations noted.
J.4	Regularly – and at least annually, a control is made of whether all data subjects have received the description of the data subject's right to insight into, correction, or erasure of personal data.	We have inquired into whether TimeLog is responsible for the duty of disclosure.	We have been informed, that TimeLog is not responsible for the duty of disclosure. No deviations noted.

Control objective K – List of processing activities

Procedures and controls are complied with, to ensure that the data processor is keeping a list of processing activity categories, processed on behalf of the data controller.

No.	Data processor's control activity	Test performed by REVI-IT A/S	Result of test
K.1	The data processor keeps a list of processing activity categories for the individual data controllers.	We have inspected the list and ensured that the list includes the relevant points.	No deviations noted.
K.2	Regularly – and at least annually – an assessment is made of whether the list of processing activity categories need to be updated.	We have inspected documentation that the list of processing activity categories for the individual data controllers is updated and correct.	No deviations noted.
K.3	Management has ensured, that the list of processing activity categories for the individual data controllers is adequate, updated and correct.	We have inspected documentation that the management has ensured that the list of processing activity categories for the individual data controllers is adequate, updated and correct.	No deviations noted.